

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Alfred Kobsa

*University of California, Irvine, CA, USA*

Friedemann Mattern

*ETH Zurich, Switzerland*

John C. Mitchell

*Stanford University, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz

*University of Bern, Switzerland*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Germany*

Madhu Sudan

*Microsoft Research, Cambridge, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbruecken, Germany*

Yang Xiang Javier Lopez C.-C. Jay Kuo  
Wanlei Zhou (Eds.)

# Cyberspace Safety and Security

4th International Symposium, CSS 2012  
Melbourne, Australia, December 12-13, 2012  
Proceedings



Springer

## Volume Editors

Yang Xiang  
Wanlei Zhou  
Deakin University  
221 Burwood Highway  
Burwood, VIC 3125, Australia  
E-mail: {yang, wanlei}@deakin.edu.au

Javier Lopez  
University of Malaga  
Campus de Teatinos  
29170 Malaga, Spain  
E-mail: jlm@lcc.uma.es

C.-C. Jay Kuo  
University of Southern California  
3740 McClintock Ave.  
Los Angeles, CA 90089-2564, USA  
E-mail: cckuo@sipi.usc.edu

ISSN 0302-9743 e-ISSN 1611-3349  
ISBN 978-3-642-35361-1 e-ISBN 978-3-642-35362-8  
DOI 10.1007/978-3-642-35362-8  
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012953043

CR Subject Classification (1998): K.6.5, D.4.6, C.2, K.4-5, E.3, I.2

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 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)

# Message from CSS 2012 General Chairs

We are privileged and delighted to welcome you to the proceedings of the 4th International Symposium on Cyberspace Safety and Security (CSS 2012).

A large fraction of the world population now spends a great deal of time in cyberspace. Cyberspace has become a critical infrastructure that is, itself, embedded in almost all other critical infrastructures and enables every aspect of human society. It is thus very much in the public interest to have a safe and secure cyberspace. The CSS 2012 conference was organized and hosted by Deakin University, Australia. Previously, CSS was held in Milan, Italy (2011), Chengdu, China (2009), and Sydney, Australia (2008).

We sincerely thank all those people who helped to organize CSS 2012. We would also like to thank the Program Chairs, Javier Lopez, University of Malaga, Spain, C.-C. Jay Kuo, University of Southern California, USA, and Yang Xiang, Deakin University, Australia, for their leadership in providing the excellent technical program. We are also grateful to the members of our Program Committee and other reviewers for their hard work in helping us produce this year's exciting program.

December 2012

Wanlei Zhou  
Peter Mueller  
Jiankun Hu

# Message from CSS 2012 Program Chairs

A warm welcome to the proceedings of the 4th International Symposium on Cyberspace Safety and Security (CSS 2012).

In the past several years, there has been a large number of attacks in cyberspace, such as attacks on the Internet, attacks on embedded/real-time computing and control systems, and attacks on dedicated computing facilities. Many research efforts have been made to achieve cyberspace safety and security, such as blocking and limiting the impact of compromise, enabling accountability, promoting deployment of defense systems, and deterring potential attackers and penalizing attackers.

In this context, we focused our program on cyberspace safety and security, such as authentication, access control, availability, integrity, privacy, confidentiality, dependability, and sustainability issues of cyberspace. The aim of this symposium is to provide a leading-edge forum to foster interaction between researchers and developers in the cyberspace safety and security communities, and to give attendees an opportunity to network with experts in this area. The symposium is a highly focused, professional, high-quality, and social event.

In response to the CSS 2012 call for papers, we received 105 submissions from 255 authors of 27 countries in the world. These papers were evaluated on the basis of their originality, significance, correctness, relevance, and technical quality. Each paper was reviewed by at least three members of the Program Committee. Based on these evaluations, of the papers submitted, 30 regular papers were selected for presentation at the conference, representing a 28.6% of acceptance rate. As the topics of this symposium are highly related to the most recent research and development of industry, we also invited seven papers from industry to be included in the program.

We would like to thank the Program Committee members and additional reviewers from all around the world for their efforts in reviewing the large number of papers. We appreciate all the associated Workshop Chairs for their dedication and professionalism. We would like to extend our sincere thanks to Wanlei Zhou, Deakin University, Australia, Peter Mueller, IBM Zurich Research, Switzerland, and Jiankun Hu, UNSW@ADFA, Australia. They provided us with invaluable guidance throughout the process of paper selection and program organization. We also thank Yu Wang for his help on completing the final proceedings.

Last but not least, we would like to take this opportunity to thank all the authors for their submissions to CSS 2012. Many of them travelled a considerable distance to participate in the conference.

December 2012

Javier Lopez  
C.-C. Jay Kuo  
Yang Xiang

# Organization

## General Chairs

Wanlei Zhou	Deakin University, Australia
Peter Mueller	IBM Zurich Research, Switzerland
Jiankun Hu	UNSW@ADFA, Australia

## Program Chairs

Javier Lopez	University of Malaga, Spain
C.-C. Jay Kuo	University of Southern California, USA
Yang Xiang	Deakin University, Australia

## Publicity Chairs

Roberto Di Pietro	Roma Tre University of Rome, Italy
Al-Sakib Khan Pathan	International Islamic University, Malaysia

## Local Arrangements Chair

Yini Wang	Deakin University, Australia
-----------	------------------------------

## Program Committee

Rafael Accorsi	University of Freiburg, Germany
Claudio Ardagna	Università degli Studi di Milano, Italy
Carlo Blundo	University of Salerno, Italy
Marco Casassa-Mont	HP Labs, UK
David Chadwick	University of Kent, UK
Frederic Cuppens	Enst Bretagne, France
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Roberto Di Pietro	Università di Roma - La Sapienza, Italy
Jose M. Fernandez	Polytechnique Montreal, Canada
Simone Fisher-Huebner	Karlstad University, Sweden
Keith Frikken	Miami University, USA
Steven Furnell	University of Plymouth, UK
Alban Gabillon	University of French Polynesia, French Polynesia
Clemente Galdi	University of Naples "Federico II", Italy

Dieter Gollmann	University of Hamburg, Germany
Juan Gonzalez Nieto	Queensland University of Technology, Australia
Yong Guan	Iowa State University, USA
Michael Huth	Imperial College London, UK
Audun Josang	University of Oslo, Norway
Sokratis Katsikas	University of Piraeus, Greece
Stefan Katzenbeisser	Technische Universität Darmstadt, Germany
Khurram Khan	King Saud University, Saudi Arabia
Shinsaku Kiyomoto	KDDI R&D Labs, Japan
Costas Lambrinouidakis	University of Piraeus, Greece
Yingjiu Li	Singapore Management University, Singapore
Jay Ligatti	University of South Florida, USA
Masahiro Mambo	Kanazawa University, Japan
Fabio Martinelli	CNR, Italy
Chris Mitchell	University of London Royal Holloway, UK
Yi Mu	University of Wollongong, Australia
Priyadarsi Nanda	University of Technology, Sydney, Australia
Stefano Paraboschi	University of Bergamo, Italy
Udaya Parampalli	University of Melbourne, Australia
Gerardo Pelosi	Politecnico di Milano, Italy
Rodrigo Roman	Institute for Infocomm Research, Singapore
Dharmendra	Sharma, University of Canberra, Australia
Nicolas Sklavos	Technological Educational Institute of Patras, Greece
Willy Susilo	University of Wollongong , Australia
Juan Tapiador	Universidad Carlos III de Madrid, Spain
Weichao Wang	UNC Charlotte, USA
Paul Watters	University of Ballarat, Australia
Sencun Zhu	Penn State University, USA

## Additional Reviewers

Firas Al Khalil	Nino Vincenzo Verde
Gianpiero Costantino	Daniele Sgandurra
Sebastien Chabrier	Alessandro Barenghi
Donald Ray	Stefano Guarino
Aliaksandr Lazouski	Peter Lee
Peter Lee	Alireza Sadighian
Alessandro Barenghi	Guillermo Suarez-Tangil
Anyi Liu	Alireza Sadighian
Dimitris Geneiatakis	Tobias Pulls
Stefano Guarino	Donald Ray
Donald Ray	Prokopios Drogkaris
Antoine Lemay	Philipp Winter
Artsiom Yautsiukhin	Antonio Villani

# Table of Contents

## CSS 2012 Regular Papers

### Session 1: Mobile Security

M-Identity and Its Authentication Protocol for Secure Mobile Commerce Applications . . . . .	1
<i>Fengling Han and Ron van Schyndel</i>	
SafeCode – Safeguarding Security and Privacy of User Data on Stolen iOS Devices . . . . .	11
<i>Avinash Srinivasan and Jie Wu</i>	
Protection Aspects of Iconic Passwords on Mobile Devices . . . . .	21
<i>Alexandre M. Braga, Rafael Cividanes, Ismael Ávila, and Claudia Tambascia</i>	
Detecting Control Flow in Smartphones: Combining Static and Dynamic Analyses . . . . .	33
<i>Mariem Graa, Nora Cuppens-Boulahia, Frédéric Cuppens, and Ana Cavalli</i>	

### Session 2: Cyberspace Attacks and Defense

A Multi-tier Ensemble Construction of Classifiers for Phishing Email Detection and Filtering . . . . .	48
<i>Jemal Abawajy and Andrei Kelarev</i>	
Chattering-Free Terminal Sliding-Mode Observer for Anomaly Detection . . . . .	57
<i>Yong Feng, Bo Wang, Fengling Han, Xinghuo Yu, and Zahir Tari</i>	
Detecting Illicit Drugs on Social Media Using Automated Social Media Intelligence Analysis (ASMIA) . . . . .	66
<i>Paul A. Watters and Nigel Phair</i>	
Improving Content Availability in the I2P Anonymous File-Sharing Environment . . . . .	77
<i>Juan Pablo Timpanaro, Isabelle Chrisment, and Olivier Festor</i>	

### Session 3: Security Applications and Systems

V2GPriv: Vehicle-to-Grid Privacy in the Smart Grid . . . . .	93
<i>Mark Stegelmann and Dogan Kesdogan</i>	



A Secure Architecture for Smart Meter Systems ..... 108  
*Daniel Angermeier, Konstantin Böttinger, Andreas Ibing,  
 Dieter Schuster, Frederic Stumpf, and Dirk Wacker*

A Novel Identity-Based Key Management and Encryption Scheme  
 for Distributed System..... 123  
*Geng Yang, Qiang Zhou, Xiaolong Xu, Jian Xu, and Chunming Rong*

An Anomaly Based Approach for HID Attack Detection Using  
 Keystroke Dynamics..... 139  
*Ferdous A. Barbhuiya, Tonmoy Saikia, and Sukumar Nandi*

Robust Authentication of Public Access Points Using Digital  
 Certificates – A Novel Approach ..... 153  
*Avinash Srinivasan and Lashidhar Chennupati*

**Session 4: Network and Cloud Security**

A General Transformation from KP-ABE to Searchable Encryption .... 165  
*Han Fei, Qin Jing, Zhao Huawei, and Hu Jiankun*

Supporting Security and Consistency for Cloud Database ..... 179  
*Luca Ferretti, Michele Colajanni, and Mirco Marchetti*

Proxy Re-encryption in a Privacy-Preserving Cloud Computing DRM  
 Scheme ..... 194  
*Ronald Petrlic*

Collaborative Behavior Visualization and Its Detection by Observing  
 Darknet Traffic ..... 212  
*Satoru Akimoto, Yoshiaki Hori, and Kouichi Sakurai*

SSH – Somewhat Secure Host ..... 227  
*Craig Valli*

**Session 5: Security Models**

Physical Access Control Administration Using Building Information  
 Models ..... 236  
*Nimalaprakasan Skandhakumar, Farzad Salim, Jason Reid, and  
 Ed Dawson*

Multiple Factors Based Evaluation of Fingerprint Images Quality ..... 251  
*Yongming Yang, Zulong Zhang, Fengling Han, and Kunming Lin*

A Leakage-Resilient Zero Knowledge Proof for Lattice Problem ..... 265  
*Yang Liu, Hongda Li, and Qihua Niu*

MDSE@R: Model-Driven Security Engineering at Runtime . . . . .	279
<i>Mohamed Almorsy, John Grundy, and Amani S. Ibrahim</i>	

## Session 6: Wireless Security

A Hash Chains Based Key Management Scheme for Wireless Sensor Networks . . . . .	296
<i>Huawei Zhao, Jing Qin, Minglei Shu, and Jiankun Hu</i>	
An Event-Based Packet Dropping Detection Scheme for Wireless Mesh Networks . . . . .	309
<i>Anderson Morais and Ana Cavalli</i>	
A State-Aware RFID Privacy Model with Reader Corruption . . . . .	324
<i>Kaleb Lee, Juan Gonzalez Nieto, and Colin Boyd</i>	
An Improved Anti-collision Algorithm for ISO15693 RFID Systems . . . . .	339
<i>Leyi Shi, Xiaorui Wang, Wenjing Fu, Xin Liu, and Zhen Qin</i>	

## Session 7: Security Protocols

Near-Optimal Collusion-Secure Fingerprinting Codes for Efficiently Tracing Illegal Re-distribution . . . . .	352
<i>Xin-Wen Wu and Alan Wee-Chung Liew</i>	
A Forward-Secure Certificate-Based Signature Scheme in the Standard Model . . . . .	362
<i>Jiguo Li, Yichen Zhang, and Huiyun Teng</i>	
Policy-Based Vulnerability Assessment for Virtual Organisations . . . . .	377
<i>Jan Muhammad, Thomas Doherty, Sardar Hussain, and Richard Sinnott</i>	
Constant-Ciphertext-Size Dual Policy Attribute Based Encryption . . . . .	400
<i>Atsuko Miyaji and Phuong V.X. Tran</i>	

## Session 8: Industry Track: Future of Cyberspace Security and Safety

Sophisticated Phishers Make More Spelling Mistakes: Using URL Similarity against Phishing . . . . .	414
<i>Max-Emanuel Maurer and Lukas Höfer</i>	
Secure Mobility Management Based on Session Key Agreements . . . . .	427
<i>Younchan Jung and Enrique Festijo</i>	

Taxonomy and Proposed Architecture of Intrusion Detection and Prevention Systems for Cloud Computing . . . . .	441
<i>Ahmed Patel, Mona Taghavi, Kaveh Bakhtiyari, and Joaquim Celestino Júnior</i>	
Portability Evaluation of Cryptographic Libraries on Android Smartphones . . . . .	459
<i>Alexandre M. Braga and Erick N. Nascimento</i>	
Secure Middleware Patterns . . . . .	470
<i>Eduardo B. Fernandez and Anton V. Uzunov</i>	
Intrusion Detection Using Disagreement-Based Semi-supervised Learning: Detection Enhancement and False Alarm Reduction . . . . .	483
<i>Yuxin Meng and Lam-for Kwok</i>	
Towards Effective Algorithms for Intelligent Defense Systems . . . . .	498
<i>Michael N. Johnstone and Andrew Woodward</i>	
<b>Author Index</b> . . . . .	509