

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

Christos Xenakis Stephen Wolthusen (Eds.)

Critical Information Infrastructures Security

5th International Workshop, CRITIS 2010
Athens, Greece, September 23-24, 2010
Revised Papers

Volume Editors

Christos Xenakis

University of Piraeus, Department of Digital Systems
Karaoli and Dimitriou 80, PC 18534 Piraeus, Greece
E-mail: xenakis@unipi.gr

Stephen Wolthusen

University of London, Department of Mathematics, Information Security Group
Royal Holloway, Egham, Surrey TW20 0EX, UK

E-mail: stephen.wolthusen@rhul.ac.uk

and

Gjovik University College, Department of Computer Science
Norwegian Information Security Laboratory

2802 Gjovik, Oppland, Norway

E-mail: stephen.wolthusen@hig.no

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-21693-0

e-ISBN 978-3-642-21694-7

DOI 10.1007/978-3-642-21694-7

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011929369

CR Subject Classification (1998): K.6.5, E.3, B.4.5, C.2, D.4.6, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2011

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

The present volume contains the carefully revised proceedings of the 5th International Workshop on Critical Information Infrastructures Security (CRITIS 2010), held during September 23–24, 2010, in Crown Plaza Athens City Hotel, Greece. The workshop was organized by the Department of Digital Systems, University of Piraeus, Greece, in conjunction with the European PKI (EuroPKI 2010) workshop and the European Research Consortium in Informatics and Mathematics’ (ERCIM) Security and Trust Management (STM 2010) workshop, and took place just after the 2010 European Symposium on Research in Computer Security (ESORICS 2010), which was also held in Athens (September 20–22). By doing so, it was facilitated to bring together not only researchers of the critical infrastructures community, but also of adjacent research communities. This continuation of the series of successful CRITIS workshops has once again allowed the research and stakeholder community from academia, research institutions, industry, and government entities to meet and exchange views covering the key areas facing critical infrastructure protection. This was reflected in the carefully selected full research papers, but also in panel discussions and the poster talks. To this end, each of the 12 out of 30 submissions was peer-reviewed anonymously by at least three independent technical experts before presentation, and the research papers contained in this volume further reflect the feedback and discussions at the workshop. Similar care was also applied to the two poster presentations; the research papers on which these were based are also included in the present volume, but marked as poster papers.

The joint format of the workshops facilitated the invitation of speakers from the critical infrastructures community, and provided a wide-ranging but topical choice of invited talks by distinguished speakers. We were fortunate to have a talk on “Data Privacy in Outsourcing Scenarios” by Pierangela Samarati of the Department of Information Technologies at the University of Milan on the first day, with the second-day keynote provided by Gustav Kalbe, the Deputy Head of Unit Trust and Security at the European Commission discussing the European policy on trust and security with a particular perspective on upcoming research and development in the 8th Framework Programme, while the third day’s keynote talk on “Enhancing Europe’s Critical Information Infrastructures—ENISA’s Resilience and CIIP Program” was given by Udo Helmbrecht, the European Network and Information Security Agency’s (ENISA) Executive Director. We would like to once again express our gratitude to these keynote speakers.

The CRITIS workshop was, moreover, able to host a special session organized by ENISA, during which Demosthenes Ikononou of ENISA provided an overview on the activities of ENISA in the areas of technologies with the potential to enhance resilience. This session also included a review of a cyber-security and cyber-warfare exercise conducted in Greece, by Dimitris Gritzalis of the

Department of Informatics, Athens University of Economics and Business, entitled “Cyberwar Ante Portas! Identifying the Role of the Academic Community in National Cyber Defense Exercises,” as well as a talk by Piotr Cholda of the Department of Telecommunications, AGH University of Science and Technology, on resilience metrics followed by a spirited panel discussion.

A year that has seen the security of control systems and particularly their use in cyber-warfare become a major concern even in mainstream media with the widespread propagation of the *Stuxnet* worm has validated many of the concerns that have been discussed in the critical infrastructure protection community for a long time, and it remains to be hoped that the problems identified in the research arena and discussed over the course of the workshop will be acted upon in a timely manner so as to prevent major incidents. It is precisely this combination of blue-skies research and analysis with more pragmatic technical solutions and engagement with stakeholders that makes the CRITIS workshops valuable to the community, and we hope that the 2010 instance was only one in what will continue to be a primary venue for this community both within its customary base in Europe and beyond.

Realizing such a workshop, however, does not happen in a vacuum, and it is first and foremost the authors and workshop participants with their original research contributions and interactions with speakers and panelists that shape the character and success of the CRITIS workshops. We would also like to thank the Technical Program Committee members whose timely and thorough reviews helped ensure not only the high quality of the research contributions, but also provided valuable insights to authors. The General Chairs, Javier Lopez of the University of Malaga and Sokratis Katsikas of the University of Piraeus, provided important guidance and stability as did the members of the standing CRITIS Steering Committee. Finally, Eleni Darra and Nikos Vrakas contributed to the successful organization of the workshop by serving as the Local Arrangements Chairs.

September 2010

Christos Xenakis
Stephen Wolthusen

VIII Organization

Lambrinoudakis Costas	University of Piraeus, Greece
Lansard Pierre-Dominique	France Telecom, France
Lewis Paul	Technology Strategy Board, UK
Luijff Eric	TNO Defence Security and Safety, The Netherlands
Masera Marcelo	EU Joint Research Centre, EU Commission
Nadjm-Tehrani Simin	Linköping University, Sweden
Ntantogian Christoforos	University of Athens, Greece
Okamoto Eiji	University of Tsukuba, Japan
Panzieri Stefano	Università di Roma Tre, Italy
Rannenber Kai	Goethe University Frankfurt, Germany
Rome Erich	Fraunhofer IAIS, Germany
Sanders William	University of Illinois, USA
Setola Roberto	Università CAMPUS Bio-Medico, Italy
Shenoi Sujeet	University of Tulsa, USA
Solms Sebastian	University of Johannesburg, South Africa
Suri Neeraj	TU Darmstadt, Germany
Suter Manuel	ETH Center for Security Studies Zurich, Switzerland
Svendsen Nils	Gjøvik University College, Norway
Taute Barend	Council for Scientific and Industrial Research, South Africa
Trushell Paul	Attorney General's Department, Australia
Tsoumas Bill	Ernst & Young and Athens University of Economics and Business, Greece
Zhou Jianying	Institute for Infocom Research, Singapore

Table of Contents

Inter-dependency Assessment in the ICT-PS Network: The MIA Project Results	1
<i>Emiliano Casalicchio, Sandro Bologna, Luigi Brasca, Stefano Buschi, Emanuele Ciapessoni, Gregorio D'Agostino, Vincenzo Fioriti, and Federico Morabito</i>	
A Quantitative Risk Analysis Approach for Deliberate Threats	13
<i>Nikos Vavoulas and Christos Xenakis</i>	
The EU FP6 Integrated Project IRRIS on Dependent Critical Infrastructures: Summary and Conclusions	26
<i>Rüdiger Klein</i>	
Towards Understanding Recurring Large Scale Power Outages: An Endogenous View of Inter-organizational Effects	43
<i>Finn Olav Sveen, Josune Hernantes, Jose J. Gonzalez, and Eliot Rich</i>	
Early Warning System for Cascading Effect Control in Energy Control Systems	55
<i>Cristina Alcaraz, Angel Balastegui, and Javier Lopez</i>	
Emergency Response with Proactive Crowd-Sourcing Reverse-111	67
<i>Anu Vaidyanathan</i>	
Anonymity and Privacy in Distributed Early Warning Systems	81
<i>Martin Brunner, Hans Hofinger, Christopher Roblee, Peter Schoo, and Sascha Todt</i>	
A Formal Adversary Capability Model for SCADA Environments	93
<i>Thomas Richard McEvoy and Stephen D. Wolthusen</i>	
A Cloud Provider-Agnostic Secure Storage Protocol	104
<i>Nikos Virvilis, Stelios Dritsas, and Dimitris Gritzalis</i>	
State-Based Firewall for Industrial Protocols with Critical-State Prediction Monitor	116
<i>Igor Nai Fovino, Andrea Carcano, Alessio Coletta, Michele Guglielmi, Marcelo Maserà and Alberto Trombetta</i>	
A Formally Verified Mechanism for Countering SPIT	128
<i>Yannis Soupionis, Stylianos Basagiannis, Panagiotis Katsaros, and Dimitris Gritzalis</i>	

Trust and Reputation for Information Exchange in Critical Infrastructures	140
<i>Filipe Caldeira, Edmundo Monteiro, and Paulo Simões</i>	
A Modelling Approach for Interdependency in Digital Systems-of-Systems Security - Extended Abstract	153
<i>Adedayo Adetoye, Sadie Creese, Michael Goldsmith, and Paul Hopkins</i>	
Risk Ontology and Service Quality Descriptor Shared among Interdependent Critical Infrastructures	157
<i>Matthieu Aubigny, Carlo Harpes, and Marco Castrucci</i>	
Author Index	161