

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 of Computer Science, Saarbruecken, Germany

Erich Rome Robin Bloomfield (Eds.)

Critical Information Infrastructures Security

4th International Workshop, CRITIS 2009
Bonn, Germany, September 30 – October 2, 2009
Revised Papers

Volume Editors

Erich Rome
Fraunhofer IAIS
53754 Sankt Augustin, Germany
E-mail: erich.rome@iais.fraunhofer.de

Robin Bloomfield
City University, London, Centre for Software Reliability
Northampton Square, London, EC1V 0HB, UK
E-mail: reb@csr.city.ac.uk

Library of Congress Control Number: 2010930333

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-14378-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-14378-6 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

© Springer-Verlag Berlin Heidelberg 2010
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

This volume contains the proceedings of the 4th International Workshop on Critical Information Infrastructures Security (CRITIS 2009). The workshop was held from September 30 to October 2 in the Günnewig Hotel Bristol in Bonn, Germany. The workshop was organized by the Fraunhofer Institute for Intelligent Analysis and Information Systems (IAIS), Sankt Augustin, Germany.

CRITIS 2009 continued the series of successful CRITIS Workshops. Companies, research institutions, and governmental organizations from all main areas of critical infrastructures took an active part in supporting CRITIS and we found CRITIS 2009 both exciting and informative. The selected papers addressed a range of key issues and demonstrated the ubiquity and global importance of information infrastructures. Each paper had at least three independent technical reviews and we accepted 13 full papers out of 34 submissions.

We were very fortunate in having a range of invited speakers that covered policy, research and industry perspectives. James Smith from Los Alamos National Laboratory addressed the challenges and achievements in their work on “Large-Scale Modeling and Simulation of Critical Infrastructure.” Orestis Terzidis, Vice President SAP AG, talked on the “The Internet for Energy: Perspectives and Challenges.” Continuing with the energy theme, Alla Heidenreich, from SIEMENS AG, Corporate Research and Technologies (Germany) provided her insights on the “Secure ICT Infrastructure for the Future Power Grid.”

Critical infrastructure protection is an area where an effective private–public partnership is required. A government perspective was provided by Michael Pilgermann, German Ministry of the Interior, who talked on German strategy regarding CIIP. Another important perspective on the partnership was provided by Paul Nicholas, Director of Global Security Strategy, Trustworthy Computing, Microsoft Corporation, who discussed “Reliance, Risk and Resiliency and the Role of Public Private Partnerships” and the changes required in how governments and industry partners understand risk, improve deterrence, respond to incidents and promulgate trust across the ICT ecosystems.

A successful workshop relies on many people. We would like to express our gratitude to all the members of the IPC who provided us with over three reviews per paper and were crucial to establishing the technical quality of the event. In addition the Local Arrangements Chairs, Rüdiger Klein and Uwe Beyer, of Fraunhofer IAIS, Germany were instrumental in providing the critical infrastructure for the workshop itself. We appreciated the overall guidance from our General Chairs Stefan Wrobel, Fraunhofer IAIS and University Bonn, Germany and Costas Lambrinoudakis, University of the Aegean, Greece and the input from the Sponsorship Chair, Bernhard Hämmerli, Hochschule Luzern, Switzerland.

In times of a global economic crisis, the Sponsorship Chair had a difficult task to perform. We are happy that we were able to win the companies IABG and Elsevier, as well as the DIESIS project, as official sponsors of CRITIS 2009 and that we received ideal support from IFIP, JRC, and the German Federal Office for Information Security, too. This support is gratefully acknowledged, as is the effort of the Sponsorship Chair Bernhard Hämmerli.

CRITIS 2009 was a truly international event, attracting 67 authors and participants from all over the world, though – not surprisingly – Europeans had the majority. Interestingly, C(I)IP is not exclusively a concern of developed countries. A number of papers from developing countries were presented at CRITIS 2009. For instance, a case study from South Africa demonstrated an effective method for assessing C(I)IP possibilities particularly for developing countries with less developed infrastructures and smaller budgets for their protection.

We very much valued the variety of talks and discussions at CRITIS 2009 and hope that these proceedings provide a lasting insight into the contribution of the workshop to understanding critical information infrastructures.

February 2010

Erich Rome
Robin Bloomfield

CRITIS 2009

Fourth International Workshop on
Critical Information Infrastructures Security

Günnewig Hotel Bristol
Bonn, Germany
September 30 – October 2, 2009

Organized by

Fraunhofer Institute for Intelligent Analysis and Information Systems (IAIS)

Program Co-chairs

Erich Rome
Robin Bloomfield

Fraunhofer IAIS, Germany
City University London and Adelard LLP, UK

General Chairs

Stefan Wrobel
Costas Lambrinoudakis

Fraunhofer IAIS and University of Bonn,
Germany
University of the Aegean, Greece

Sponsorship Chair

Bernhard M. Hämmerli

Acris GmbH & University of Applied Sciences
Lucerne, Switzerland

Local Organization Chairs

Uwe Beyer
Rüdiger Klein

Fraunhofer IAIS, Germany
Fraunhofer IAIS, Germany

International Program Committee

Fabrizio Baiardi
Sandro Bologna
Stefan Brem

Università di Pisa, Italy
ENEA, Italy
Swiss Federal Department of Defense, Civil
Protection and Sport, Switzerland
Università di Tor Vergata Rome, Italy
Telecom Italia, Italy

Emiliano Casalicchio
Roberto Clemente

VIII Organization

Geert Deconinck	Katholieke Universiteit Leuven, Belgium
Giovanna Dondossola	Cesi Ricerca, Italy
Myriam Dunn	ETH Center for Security Studies Zurich, Switzerland
Erol Gelenbe	Imperial College London, UK
Stefan Geretshuber	IABG, Germany
Adrian Gheorghe	Old Dominion University, USA
Stefanos Gritzalis	University of the Aegean, Greece
Nouredine Hadjsaid	L.E.G. – Grenoble Institute of Technology, France
Bernhard M. Hämmerli	Acris GmbH & University of Applied Sciences Lucerne, Switzerland
Rüdiger Klein	Fraunhofer IAIS, Germany
Pierre-Dominique Lansard	France Telecom, France
Paul Lewis	Network Security Innovation Platform, UK
Javier Lopez	University of Malaga, Spain
Eric Luijijf	TNO Defence Security and Safety, The Netherlands
Marcelo Masera	Joint Research Centre European Commission, Institute for the Protection and Security of the Citizen, Italy
Simin Nadjm-Tehrani	Linköping University, Sweden
Eiji Okamoto	University of Tsukuba, Japan
Ciaran Osborn	Centre for the Protection of National Infrastructure, UK
Dirk Reinermann	BSI, Germany
Roberto Setola	Università CAMPUS Bio-Medico, Italy
Sujeet Shenoj	University of Tulsa, USA
Neeraj Suri	TU Darmstadt, Germany
Salvatore Tucci	Università di Tor Vergata Rome, Italy
Paulo Verissimo	Universidade de Lisboa, Portugal
Stephen D. Wolthusen	Royal Holloway, University of London, UK, UK & Gjøvik University College, Norway
Stefan Wrobel	University of Bonn and Fraunhofer IAIS, Germany
Jianying Zhou	Institute for Infocom Research, Singapore

Local Organization Committee

Birgit Dorn, Yvonne Grabowski, Torsten Heinrich, Achim Kapusta, Christine Malich, Ulrich Nütten, Daniela Plath	Fraunhofer IAIS, Germany
--	--------------------------

Steering Committee

Chairs

Bernhard M. Hämmerli

Acris GmbH & University of Applied Sciences
Lucerne, Switzerland

Javier Lopez

University of Malaga, Spain

Stephen D. Wolthusen

Royal Holloway University, UK & Gjøvik
University College Norway

Members

Sandro Bologna

ENEA CR-Casaccia, Rome, Italy

Sokratis Katsikas

University of Piraeus, Greece

Erich Rome

Fraunhofer IAIS, Germany

Roberto Setola

Università Campus BioMedico Roma, Italy

Table of Contents

On Modelling of Inter-dependent Network Infrastructures by Extended Leontief Models	1
<i>Gregorio D'Agostino, Roberto Cannata, and Vittorio Rosato</i>	
Critical Infrastructure Protection in Brazil - Threat Identification and Analysis	14
<i>João H.A. Franco, Sérgio L. Ribeiro, Sandra M.C. Tome, Christiane M.S. Cuculo, Marcos B. Trindade, Leonardo M. Lage, and Regina M.F. Souza</i>	
Development of Information Security-Focused Incident Prevention Measures for Critical Information Infrastructure in Japan	22
<i>Hideaki Kobayashi, Kenji Watanabe, Takahito Watanabe, and Yukinobu Nagayasu</i>	
Design of a Mobile Agent-Based Adaptive Communication Middleware for Federations of Critical Infrastructure Simulations	34
<i>Gökçe Görbil and Erol Gelenbe</i>	
An Alternate Topology Generator for Joint Study of Power Grids and Communication Networks	50
<i>Alpha Amadou Diallo and Claude Chaudet</i>	
Trouble Brewing: Using Observations of Invariant Behavior to Detect Malicious Agency in Distributed Control Systems	62
<i>Thomas Richard McEvoy and Stephen D. Wolthusen</i>	
Optimisation of Critical Infrastructure Protection: The SiVe Project on Airport Security	73
<i>Marcus Breiing, Mara Cole, John D'Avanzo, Gebhard Geiger, Sascha Goldner, Andreas Kuhlmann, Claudia Lorenz, Alf Papproth, Erhard Petzel, and Oliver Schwetje</i>	
Cyber-Critical Infrastructure Protection Using Real-Time Payload-Based Anomaly Detection	85
<i>Patrick Düssel, Christian Gehl, Pavel Laskov, Jens-Uwe Bußer, Christof Störmann, and Jan Kästner</i>	
Decision Aid Tool and Ontology-Based Reasoning for Critical Infrastructure Vulnerabilities and Threats Analysis	98
<i>Michał Choraś, Adam Flizikowski, Rafał Kozik, and Witold Hołubowicz</i>	

Application Filters for TCP/IP Industrial Automation Protocols 111
*Aguinaldo B. Batista Jr., Tiago H. Kobayashi,
João Paulo S. Medeiros, Agostinho M. Brito Jr., and
Paulo S. Motta Pires*

Web Browser Security Update Effectiveness 124
Thomas Duebendorfer and Stefan Frei

State-Based Network Intrusion Detection Systems for SCADA
Protocols: A Proof of Concept 138
*Andrea Carcano, Igor Nai Fovino, Marcelo Masera, and
Alberto Trombetta*

Towards Early Warning Systems – Challenges, Technologies and
Architecture 151
Martin Apel, Joachim Biskup, Ulrich Flegel, and Michael Meier

CII Protection - Lessons for Developing Countries: South Africa as a
Case Study 165
Mboneli Ndlangisa and Deon Herbst

Energy Theft in the Advanced Metering Infrastructure 176
Stephen McLaughlin, Dmitry Podkuiko, and Patrick McDaniel

Current Capabilities, Requirements and a Proposed Strategy for
Interdependency Analysis in the UK 188
Robin Bloomfield, Nick Chozos, and Kizito Salako

Stochastic Modelling of the Effects of Interdependencies between
Critical Infrastructure 201
*Robin Bloomfield, Lubos Buzna, Peter Popov, Kizito Salako, and
David Wright*

Author Index 213