Lecture Notes in Computer Science 7130

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

Javier Lopez Roberto Setola
Stephen D. Wolthusen (Eds.)

Critical Infrastructure Protection

Information Infrastructure Models, Analysis, and Defense

Springer

Volume Editors

Javier Lopez
University of Malaga
Computer Science Department
29071 Malaga, Spain
E-mail: jlm@lcc.uma.es

Roberto Setola
University CAMPUS Bio- Medico di Roma
Complex Systems and Security Lab
Via Alavro del Portillo, 21
00128 Roma, Italy
E-mail: r.setola@unicampus.it

Stephen D. Wolthusen
University of London
Information Security Group
Department of Mathematics
Egham, Surrey TW20 0EX, UK
and
Gjøvik University College
Norwegian Information Security Laboratory
Faculty of Computer Science
2802 Gjøvik, Norway
E-mail: stephen.wolthusen@rhul.ac.uk

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-28919-4 e-ISBN 978-3-642-28920-0
DOI 10.1007/978-3-642-28920-0
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012933456
CR Subject Classification (1998): D.4.6, K.6.5, E.3, C.2, H.4, H.3, I.6, J.1

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

Information and communication technology (ICT) systems form an integral part of critical infrastructure globally, whether in their own right or as a supporting or controlling mechanism for other sectors. Although there are large bodies of work on the safety and reliability of the underlying systems and components and on many security aspects affecting the critical infrastructure's ICT elements, there are a significant number of issues that are unique and both deserve and demand to be considered in their own right.

Although not the main focus of the present volume, it begins with an understanding of the effects and impacts of failures in the critical infrastructure including any cascading effects that may also occur in different locations or at later points in time, but also must take into account the conflict between more conventional security considerations and the often overriding imperative to ensure availability that imply a much greater reliance on a system's resilience to failure and compromise than is typically given consideration, e.g., in the development of cryptographic security mechanisms.

Moreover, the properties of critical information infrastructures make it inevitable that the inter-relationships with the physical infrastructure be considered, which can arise in many different forms from the need to satisfy hard real-time constraints to having to understand the way that a physical system state influences ICT components and vice versa.

Beyond such largely academic and technical considerations, however, the field also has a necessarily strong link to economic and policy considerations, which directly and indirectly influence any approach to the safety, security, and resilience of the critical (information) infrastructure. Recent developments have shown the need to regularly assess the validity of many explicit and tacit assumptions, including whether attacks on critical infrastructure by non-state (e.g., terrorist) or state actors ("cyber warfare") represent a genuine threat.

The present volume cannot begin to cover all of these issues in a satisfactory manner. However, in combining elementary concepts and models with policy-related issues and placing an emphasis on the timely area of control systems, the book aims to highlight some of the key issues facing the research community. The sector studies included provide further insights into selected issues encountered both in infrastructure sectors that have been studied extensively such as the electric grid, but also ones that have not seen similar attention despite their obvious significance, namely, the financial services sector, but also the oil and gas elements of the energy and the transportation sector with their reliance on ICT systems to ensure levels of efficiency and safety that would otherwise not be possible to achieve.

We hope that this book can serve as a timely introduction to the state of the art in critical infrastructure protection, particularly for the information infrastructure, and as such may aid both researchers to gain an overview of a field that is still largely dominated by conference publications and a disparate body of literature, but also lecturers wishing to prepare postgraduate-level courses in this rapidly moving and multifaceted field.

October 2011

Javier Lopez
Roberto Setola
Stephen D. Wolthusen

List of Contributors

Andreas Aas
Norwegian University of Science and Technology, Norway
E-mail: aasand@jbv.no

Cristina Alcaraz
Computer Science Department, University of Malaga, Spain
E-mail: alcaraz@lcc.uma.es

Ettore Bompard
Department of Electrical Engineering, Politecnico di Torino, Italy
E-mail: ettore.bompard@polito.it

Fernando Carvajal
INDRA, Spain
E-mail: jfcarvajal@indra.es

Paolo Cuccia
Department of Dispatching and Grid Operation, Terna S.p.A, Italy
E-mail: paolo.cuccia@terna.it

Jordi Cucurull
Department of Computer and Information Science,
Linköping University, Sweden
E-mail: g-jorcu@ida.liu.se

Myriam Dunn Cavelty
Center for Security Studies, ETH Zurich, Switzerland
E-mail: dunn@sipo.gess.ethz.ch

Gerardo Fernandez
Computer Science Department, University of Malaga, Spain
E-mail: gerardo@lcc.uma.es

Igor Nai Fovino
Institute for the Protection and Security of the Citizen, Joint Research Center,
European Commission
E-mail: igor.nai@jrc.ec.europa.eu

Andrea Glorioso
European Commission DG Information Society and Media, Unit A3 - Internet,
Network and Information Security
E-mail: Andrea.Glorioso@ec.europa.eu

Daniel Germanus
Computer Science Department, Technische Universität Darmstadt, Germany
E-mail: germanus@cs.tu-darmstadt.de

Rajni Goel
Department of Information Systems and Decision Sciences,
Howard University, USA
E-mail: rgoel@howard.edu

Stuart Goldman
USA
E-mail: familygoldman@gmail.com

Bernhard Hämmerli
Department of Computer Science, Norwegian Information Security Laboratory,
Gjøvik University Collage, Norway
E-mail: bmhaemmerli@acris.ch; E-mail: Bernhard.Hammerli@hig.no

Mark Hartong
Federal Railroad Administration, U.S. Department of Transportation, USA
E-mail: mark.hartong@dot.gov

Stig O. Johnsen
Norwegian University of Science and Technology, Norway
E-mail: Stig.O.Johnsen@gmail.com

Abdelmajid Khelil
Computer Science Department, Technische Universität Darmstadt, Germany
E-mail: khelil@cs.tu-darmstadt.de

Javier Lopez
Computer Science Department, University of Malaga, Spain
E-mail: jlm@lcc.uma.es

Eric Luiijf
Netherlands Organisation for Applied Scientific Research - TNO,
The Netherlands
E-mail: eric.luiijf@tno.nl

Marcelo Masera
Institute for Energy, Joint Research Center, European Commission
E-mail: marcelo.masera@jrc.it

Simin Nadjm-Tehrani
Department of Computer and Information Science, Linköping University,
Sweden
E-mail: simin@ida.liu.se

Ying Qian
Shanghai University, Shanghai
E-mail: iris_qian@hotmail.com

Massimiliano Raciti
Department of Computer and Information Science,
Linköping University, Sweden
E-mail: masra@ida.liu.se

Julian L. Rrushi
Faculty of Computer Science, University of New Brunswick, Canada
E-mail: jrrushi@unb.ca

Andrea Servida
European Commission DG Information Society and Media, Unit A3 - Internet, Network and Information Security
E-mail: Andrea.Servida@ec.europa.eu

Roberto Setola
Faculty of Engineering, Universitá Campus Bio-Medico di Roma, Italy
E-mail: r.setola@unicampus.it

Neeraj Suri
Computer Science Department, Technische Universität Darmstadt, Germany
E-mail: suri@cs.tu-darmstadt.de

Manuel Suter
Center for Security Studies, ETH Zurich, Switzerland
E-mail: suter@sipo.gess.ethz.ch

Nils Kalstad Svendsen
Norwegian Information Security Laboratory, Faculty of Computer Science,
Gjøvik University College, Norway
E-mail: nils.svendsen@hig.no

Huseyin Uzunalioglu
Alcatel-Lucent, USA
E-mail: huseyin.uzunalioglu@alcatel-lucent.com

Dumida Wijesekra
Department of Computer Science, George Mason University, USA
E-mail: dwijesek@gmu.edu

Stephen D. Wolthusen
Norwegian Information Security Laboratory, Faculty of Computer Science,
Gjøvik University College, Norway
E-mail: stephen.wolthusen@hig.no and
Information Security Group, Department of Mathematics, Royal Holloway,
University of London, UK
E-mail: stephen.wolthusen@hig.no

Part I
Introduction to Critical Information Infrastructure Protection

The chapters in this part provide an overview of the concepts and terminology used throughout this volume and also serve as a high-level outlook on current developments in critical information infrastructure research. As these are inevitably interlinked, the following chapters also provide a perspectives on the larger critical infrastructure area, its interactions with the policy domain, and the risks and vulnerabilities that the critical information infrastructure is exposed to.

Part II
Models and Defensive Mechanisms

In this part, the current state of research on modeling critical infrastructures is elaborated with an emphasis on information infrastructures and the associated problems of early warning and attack detection mechanisms; the latter are critical as the critical information infrastructure is typically required to operate continuously and may not easily be shut down or degraded for defensive or recovery purposes. An example of the type of models involving physical as well as ICT elements is provided in the second chapter of this part, while further aspects of this problem area will be discussed in the following Parts III and IV as well.

Part III
Control Systems and Protocols

A key part of the critical information infrastructure is in fact not immediately visible as it is embedded in automation and control systems, which are the focus of Part III. Following an introduction to the problems of supervisory control and data acquisition (SCADA) and distributed control (DCS) systems, research on vulnerability of control systems with particular emphasis on areas where differences to standard network and information systems arise is discussed followed by a review of the security threats and possible countermeasures resulting from ongoing developments away from proprietary protocols and towards open standards, along with the increased risks of inadvertent and inadvisable interconnections.

Part IV
Infrastructure Sector Studies

The final part of this volume is devoted to a selection of sector studies. These deal with two sub-sectors of the energy sector, namely the electric grid with an emphasis on the conventional, large-scale grid and its robust operation, and also the oil, gas, and petrochemical industries. In addition, a chapter on telecommunications highlights some of the concerns raised by convergent next-generation telecommunications infrastructures that have been or are being deployed by many advanced telecommunications carriers. The chapter on the financial services industry focuses largely on the back-end infrastructure of banks and institutions in the sector, but also highlights some of the problems facing the sector from new technology being deployed before a review of the transportation sector with an emphasis on a case study for the rail transportation sector.

Table of Contents