1. Record Nr. UNISA996465898503316

Titolo	Critical information infrastructures security : second international workshop, CRITIS 2007, Malaga, Spain, October 3-5, 2007 : revised papers / / Javier Lopez, Bernhard M. Hammerli (eds.)
Pubbl/distr/stampa	Berlin, Germany ; ; New York, New York : , : Springer, , [2008] ©2008
ISBN	1-283-43791-0 9786613437914 3-540-89173-0
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (XI, 362 p.)
Collana	Security and Cryptology ; ; 5141
Disciplina	005.8
Soggetti	Computers - Access control Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Session 1: R&D Agenda -- Towards a European Research Agenda for CIIP: Results from the CI2RCO Project -- ICT Vulnerabilities of the Power Grid: Towards a Road Map for Future Research -- Session 2: Communication Risk and Assurance I -- An Analysis of Cyclical Interdependencies in Critical Infrastructures -- A Framework for 3D Geospatial Buffering of Events of Interest in Critical Infrastructures -- Designing Information System Risk Management Framework Based on the Past Major Failures in the Japanese Financial Industry -- Advanced Reaction Using Risk Assessment in Intrusion Detection Systems -- Session 3: Communication Risk and Assurance II -- Managing Critical Infrastructures through Virtual Network Communities -- The Structure of the Sense of Security, Anshin -- Securing Agents against Malicious Host in an Intrusion Detection System -- Session 4: Code of Practice and Metrics -- UML Diagrams Supporting Domain Specification Inside the CRUTIAL Project -- Expert System CRIPS: Support of Situation Assessment and Decision Making -- Using Dependent CORAS Diagrams to Analyse Mutual Dependency -- A Methodology to Estimate Input-Output Inoperability Model Parameters -- Session 5: Information

Sharing and Exchange -- Efficient Access Control for Secure XML Query Processing in Data Streams -- An Approach to Trust Management Challenges for Critical Infrastructures -- Session 6: Continuity of Services and Resiliency -- Detecting DNS Amplification Attacks -- LoRDAS: A Low-Rate DoS Attack against Application Servers -- Intra Autonomous System Overlay Dedicated to Communication Resilience -- A Proposal for the Definition of Operational Plans to Provide Dependability and Security -- Session 7: SCADA and Embedded Security -- Application of Kohonen Maps to Improve Security Tests on Automation Devices -- Ideal Based Cyber Security Technical Metrics for Control Systems -- Designing Critical Infrastructure Cyber Security Segmentation Architecture by Balancing Security with Reliability and Availability -- Session 8: Threats and Attacks Modeling -- A General Model and Guidelines for Attack Manifestation Generation -- A Survey on Detection Techniques to Prevent Cross-Site Scripting Attacks on Current Web Applications -- Attack Modeling of SIP-Oriented SPIT -- A Malware Detector Placement Game for Intrusion Detection -- Session 9: Information Exchange and Modelling -- Modeling and Simulating Information Security Management -- Design of a Platform for Information Exchange on Protection of Critical Infrastructures -- Towards a Standardised Cross-Sector Information Exchange on Present Risk Factors.

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the Second International Workshop on Critical Information Infrastructures Security, CRITIS 2007, held in Benalmadena-Costa, Spain, in October 2007 in conjunction with ITCIP 2007, the first conference on Information Technology for Critical Infrastructure Protection. The 29 revised full papers presented were carefully reviewed and selected from a total of 75 submissions. The papers address all security-related heterogeneous aspects of critical information infrastructures and are organized in topical sections on R&D agenda, communication risk and assurance, code of practice and metrics, information sharing and exchange, continuity of services and resiliency, SCADA and embedded security, threats and attacks modeling, as well as information exchange and modeling.