

1. Record Nr.	UNISA996465911503316
Titolo	Critical Information Infrastructure Security [[electronic resource]] : 5th International Workshop, CRITIS 2010, Athens, Greece, September 2010, Revised Papers // edited by Christos Xenakis, Stephen Wolthusen
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2011
ISBN	3-642-21694-3
Edizione	[1st ed. 2011.]
Descrizione fisica	1 online resource (X, 161 p. 54 illus., 33 illus. in color.)
Collana	Security and Cryptology ; ; 6712
Disciplina	005.8
Soggetti	Management information systems Computer science Data encryption (Computer science) Computer software—Reusability Computer communication systems Special purpose computers Computer system failures Management of Computing and Information Systems Cryptology Performance and Reliability Computer Communication Networks Special Purpose and Application-Based Systems System Performance and Evaluation
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and author index.
Nota di contenuto	Intro -- Title page -- Preface -- Organization -- Table of Contents -- Inter-dependency Assessment in the ICT-PS Network: The MIA Project Results -- Introduction -- The MIA Framework -- Inter-dependency Models -- Topological Model -- Analytical Model -- Simulation Model -- Interdependency Metrics -- Topological Robustness -- Module and Phase of Frequency Response and the Poles Placement -- Ratio of Inter-dependency -- Temporal Scale of Inter-dependency -- Scale of Criticality -- Metrics Evaluation -- Main Project Findings --

Conclusions and Outlook -- References -- A Quantitative Risk Analysis Approach for Deliberate Threats -- Introduction -- Motivation -- Proposed Approach -- Conceptual Foundation -- The Modeling Tools -- Mathematical Foundation -- Risk Analysis Approach: Step-by-Step -- A Simple Example -- Conclusions and Future Work -- References -- The EU FP6 Integrated Project IRRIS on Dependent Critical Infrastructures Summary and Conclusions -- Introduction -- Analysis and Modeling -- The IRRIS Information Model -- Preliminary Interdependency Analysis (PIA) -- Detailed Technical Federated Simulations -- User Interactions -- Scenarios and Experiments -- Middleware Technology (MIT) -- Use Cases -- Conclusions and Lessons Learnt -- Modeling and Simulation -- User Interaction Capabilities -- Scenarios -- Other Critical Infrastructure Domains -- Middleware Improved Technology -- References -- Towards Understanding Recurring Large Scale Power Outages: An Endogenous View of Inter-organizational Effects -- Introduction -- Problem -- Hypothesis -- Analysis -- Policy and Implementation -- Conclusion -- References -- Early Warning System for Cascading Effect Control in Energy Control Systems -- Introduction -- SCADA System and Control Technologies -- SCADA Network Architecture -- WSN, An Alternative for the Control. Early Warning Systems on the Critical System Protection -- Preventing and Controlling a Cascading Effect -- Early Warning System Based on Forensic Techniques -- Use Case and Discussion -- Conclusions and Future Work -- References -- Emergency Response with Proactive Crowd-Sourcing Reverse-111 -- Introduction -- Reverse 111 - Proactive Crowd Sourcing -- System Overview -- System Architecture -- Resource Schedulers -- Greedy Scheduler -- Lottery Scheduler -- Round-Robin Scheduler -- Visualization Interface -- Evaluation -- Evaluation of Proactive Crowd-Sourcing -- Related Work -- Conclusions and Future Work -- References -- Anonymity and Privacy in Distributed Early Warning Systems -- Introduction -- Related Work -- International Activities -- Collaborative Centralised Approaches -- Distributed and Collaborative Approaches -- A Distributed Collaborative Privacy-Preserving Approach -- Design Goals -- Component Technologies -- Integration and Use Cases -- Discussion and Future Work -- Reputation Tracking -- Role of a Trusted Third Party -- Data Analysis -- Practical Implementation of the Concept -- Conclusion -- References -- A Formal Adversary Capability Model for SCADA Environments -- Introduction -- -Calculus Variant -- Model of a SCADA Network -- Agent-Based Adversary Capabilities -- Adversary Communication with SCADA Processes -- Agent Recruitment -- Covert Communication -- Message Interception and Manipulation -- Denial of Service -- Model Utility: Discussion and Example -- Related Work -- Conclusion and Future Work -- References -- A Cloud Provider-Agnostic Secure Storage Protocol -- Introduction -- Related Work -- A Confidentiality and Integrity Ensuring Model -- File Splitting -- Hybrid Encryption -- Chunks Message Authentication Code -- Index File -- Data Management -- Evaluation of Our Model -- Conclusions and Future Work -- References.

State-Based Firewall for Industrial Protocols with Critical-State Prediction Monitor -- Introduction -- Related Works -- State Analysis Filtering -- Rules Languages -- Packet Language -- Critical State Language -- Critical State Distance -- Distance Evaluation -- Experimental Tests -- Distance Performance -- Conclusions -- References -- A Formally Verified Mechanism for Countering SPIT -- Introduction -- Methodology -- Policy Description -- Policy Integration in a VoIP Environment -- Experiments -- Formal Verification -- Assumptions and Property Specification -- SIP-aSPM Model Description

-- Verification Results -- Related Work -- Conclusions -- References
-- Trust and Reputation for Information Exchange in Critical Infrastructures -- Introduction -- Related Work -- Application Scenario
-- Trust and Reputation Service -- TRS Agents -- TRS Discovery Tool
-- Validation -- Conclusions -- References -- A Modelling Approach for Interdependency in Digital Systems-of-Systems Security - Extended Abstract -- References -- Risk Ontology and Service Quality Descriptor Shared among Interdependent Critical Infrastructures -- Introduction -- Risk Description -- How to Describe Risk? -- Service Quality Descriptor -- Value Assignment to SQD -- Simplified Method of SQD Assessment -- Assumptions -- SQD Parameters Computation -- References -- Author Index.

Sommario/riassunto

This book constitutes the thoroughly refereed post-proceedings of the 5th International Workshop on Critical Information Infrastructure Security, CRITIS 2010, held in Athens, Greece in September 2010. The 12 revised full papers and two poster papers presented went through two rounds of reviewing and improvement and were selected from 30 submissions. The papers included address various techniques to realize the security of systems, communications, and data.
