1. Record Nr. UNISA996466435203316

Titolo	Critical Information Infrastructures Security [[electronic resource]] : 11th International Conference, CRITIS 2016, Paris, France, October 10–12, 2016, Revised Selected Papers / / edited by Grigore Havarneanu, Roberto Setola, Hypatia Nassopoulos, Stephen Wolthusen
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
ISBN	3-319-71368-X
Edizione	[1st ed. 2017.]
Descrizione fisica	1 online resource (XI, 348 p. 103 illus.)
Collana	Security and Cryptology ; ; 10242
Disciplina	005.8
Soggetti	Computer security Computer communication systems Architecture, Computer Computers and civilization Computers Law and legislation Microprogramming Systems and Data Security Computer Communication Networks Computer System Implementation Computers and Society Legal Aspects of Computing Control Structures and Microprogramming
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Stealth Low-Level Manipulation of Programmable Logic Controllers I/O by Pin Control Exploitation -- 1 Introduction -- 2 Background -- 2.1 Pin Control Subsystem -- 2.2 How PLCs Control the Pins -- 3 Pin Control Attack -- 3.1 Security Concerns Regarding Pin Control -- 3.2 Pin Control Attack Details -- 3.3 Threat Model -- 4 A Pin Control Attack in Practice -- 4.1 Environment Setup -- 4.2 Attack Implementation -- 5 Discussion --

5.1 Implications of Attack on the ICS -- 5.2 Detection of Pin Control Attack -- 6 Related Work -- 7 Conclusion -- References -- Developing a Cyber Incident Communication Management Exercise for CI Stakeholders -- 1 Introduction -- 1.1 Background -- 1.2 Case Study: Red Team - Blue Team Exercise -- 2 Communication Management Exercise for ICS Security (CME-ICS) -- 2.1 Peculiarity of Existing Japanese CIP Training -- 2.2 Discussion-Based Exercise -- 2.3 Theme of the Exercise: Communication Management -- 2.4 Scenario -- 2.5 Exercise Steps -- 2.6 Administration Staff -- 2.7 Pilot Exercises -- 3 Results and Discussion -- 3.1 Variation of Incident Management Structure -- 3.2 Results of the Survey -- 3.3 Discussion -- 3.4 Future Work: ``ICS-SIRT'' Exercise -- References -- On Auxiliary Entity Allocation Problem in Multi-layered Interdependent Critical Infrastructures -- 1 Introduction -- 2 Problem Formulation Using the Implicative Interdependency Model -- 3 Computational Complexity Analysis -- 3.1 Special Case: Problem Instance with One Minterm of Size One -- 3.2 General Case: Problem Instance with an Arbitrary Number of Minterms of Arbitrary Size -- 4 Solutions to the AEAP Problem -- 4.1 Optimal Solution to AEAP Problem -- 4.2 Heuristic Solution to the AEAP Problem -- 5 Experimental Results -- 6 Conclusion -- References -- Cyber Targets Water Management -- 1 Introduction.
1.1 Use of Industrial Control Systems -- 1.2 Cyber Threats and Risk -- 1.3 Structure of This Paper -- 2 Related Work -- 3 A Benchmark of the Resilience of the ICS Environment -- 4 Observed ICS Security Dilemmas -- 5 Cyber Security Simulator for Water Management Control Systems -- 5.1 Deployment of Attack Scenarios -- 5.2 DESI Results -- 6 Conclusions and Future Work -- 6.1 Future Work -- References -- Integrated Safety and Security Risk Assessment Methods: A Survey of Key Characteristics and Applications -- 1 Introduction -- 2 Related Work -- 3 Review Methodology -- 4 Integrated Safety and Security Risk Assessment Methods -- 4.1 SAHARA Method -- 4.2 CHASSIS Method -- 4.3 FACT Graph Method -- 4.4 FMVEA Method -- 4.5 Unified Security and Safety Risk Assessment Method -- 4.6 Extended CFT Method -- 4.7 EFT Method -- 5 Analysis of Integrated Safety and Security Risk Assessment Methods -- 6 Conclusions and Future Work -- References -- Railway Station Surveillance System Design: A Real Application of an Optimal Coverage Approach -- Abstract -- 1 Introduction -- 2 Railway Station Surveillance and Sensor Placement Problem -- 3 Application of the Optimal Coverage Approach to a Real Case -- 3.1 Area of Interest and Input Data -- 3.2 Coverage Analysis and Coverage Matrix -- 3.3 Modeling of the Coverage Problem and Solution of the Model -- 4 Experimental Results -- 4.1 Set Covering Model -- 4.2 Maximal Covering Model -- 5 Conclusions -- References -- A Synthesis of Optimization Approaches for Tackling Critical Information Infrastructure Survivability -- Abstract -- 1 Introduction -- 2 Identifying Critical Network Components: Survivability-Oriented Interdiction Models -- 3 Enhancing Critical Network Survivability: Resource Allocation Strategy Models -- 3.1 Optimization Models for Protecting CII Physical Components.
3.2 Optimization Models for CII Service Restoration -- 4 Planning Survivable Networks: Design Models -- 5 Future Research Suggestions -- 6 Conclusions -- References -- A Dataset to Support Research in the Design of Secure Water Treatment Systems -- 1 Introduction -- 2 Secure Water Treatment (SWaT) -- 2.1 Water Treatment Process -- 2.2 Communications -- 3 Attack Scenarios -- 4 Data Collection Process -- 4.1 Physical Properties -- 4.2 Network Traffic -- 4.3 Labelling Data -- 5 Conclusion -- References -- Human Vulnerability Mapping Facing

Critical Service Disruptions for Crisis Managers -- Abstract -- 1 Introduction -- 2 Consequence Assessment -- 3 Modelling People Mobility -- 4 Results and Interests of Mapping Human Vulnerability -- 5 Improving Human Vulnerability Assessment -- 6 Conclusion -- Acknowledgments -- References -- A Methodology for Monitoring and Control Network Design -- 1 Introduction -- 2 Related Work -- 3 Asset Risk Assessment in ICS -- 3.1 Overview of the CAIA Approach -- 3.2 Risk Assessment Based on the Impact Measures -- 4 Optimal Control Network Design -- 5 Experimental Results -- 5.1 Results on the TEP -- 5.2 Results on the IEEE 14-Bus Electricity Grid -- 5.3 Results on the IEEE 300-Bus Electricity Grid Model -- 6 Conclusions -- References -- Effective Defence Against Zero-Day Exploits Using Bayesian Networks -- 1 Introduction -- 2 Modelling and Problem Representation -- 3 Case Study and Results -- 3.1 Case Study Settings -- 3.2 Results -- Deploying a Single Control -- 3.3 Results -- Deploying Combined Controls -- 4 Related Work -- 5 Conclusion and Future Work -- References -- Power Auctioning in Resource Constrained Micro-grids: Cases of Cheating -- 1 Introduction -- 2 Related Work -- 3 Decentralised Continuous Double Auction Model -- 4 Cheating CDA Attacks -- 4.1 Case 1: Victim Strategy Downgrade -- 4.2 Case 2: Collusion Attack.
5 Sketch Countermeasures -- 6 Conclusions -- References -- Using Incentives to Foster Security Information Sharing and Cooperation: A General Theory and Application to Critical Infrastructure Protection -- 1 Introduction -- 2 Theoretical Framework and Propositions -- 2.1 Regulation Alone Cannot Solve the Free Rider Problem -- 2.2 Linking Incentives to Voluntary SIS -- 2.3 A Holistic and Multidisciplinary Approach -- 2.4 A Model Linking Incentives, Behavior, and SIS -- 2.5 Reciprocity Expectation -- 2.6 Value Expectation -- 2.7 Institutional Expectation -- 2.8 Reputation Expectation -- 2.9 The Moderating Role of Trust -- 3 Application of the Proposed Model to Critical Infrastructure Protection -- 3.1 The Swiss Reporting and Analysis Centre for Information Security -- 3.2 Reciprocity Expectation -- 3.3 Value Expectation -- 3.4 Institutional Expectation -- 3.5 Reputation Expectation -- 3.6 The Moderating Role of Trust -- 4 Discussion -- 5 Concluding Comments and Next Steps -- References -- Dynamic Risk Analyses and Dependency-Aware Root Cause Model for Critical Infrastructures -- 1 Introduction -- 2 Terminology -- 3 Risk Assessments Using the Dependency-Aware Root Cause (DARC) Model -- 4 Risk Taxonomy for Critical Infrastructures -- 4.1 Dependency Definition Language -- 4.2 Generating the Dependency Graph -- 5 The `Smart Grid Luxembourg' Use-Case -- 5.1 Compiling a Dependency-Aware Inventory -- 5.2 Threat Model -- 5.3 Generation of the Dependency Graph -- 5.4 Results -- 6 Conclusion and Future Work -- References -- Selecting Privacy Solutions to Prioritise Control in Smart Metering Systems -- 1 Introduction -- 2 Privacy and Automation Properties -- 3 Selecting Techniques: Analysis and Discussion -- 3.1 Analysis of Privacy Techniques -- 3.2 Discussion: Privacy vs. Control -- 4 Conclusions and Future Work -- References.
A Six-Step Model for Safety and Security Analysis of Cyber-Physical Systems -- 1 Introduction -- 2 Preliminaries and Background -- 2.1 CPS Safety and Security -- 2.2 GTST-MLD and the 3-Step Model -- 2.3 The SWaT System -- 3 Complex System Safety and Security Modeling: SSM -- 4 Summary and Conclusion -- References -- Availability Study of the Italian Electricity SCADA System in the Cloud -- 1 Introduction -- 1.1 The Hierarchical SCADA System -- 1.2 Cloud Deployments for a Nationwide SCADA System -- 2 Availability Computation in a Hierarchical SCADA Network -- 2.1 Availability Model for an Optical

Network -- 2.2 Availability Computation -- 3 Availability Assessment in the SCADA System Managing the Italian Electricity Grid -- 4 Conclusion -- References -- Railway System Failure Scenario Analysis -- 1 Introduction -- 2 Failure Scenario Analysis: From Power Grid to Railway -- 2.1 NESCOR Failure Scenarios for the Energy Sector -- 2.2 Toward Railway Transportation Failure Scenarios -- 3 Sample Railway System Failure Scenarios -- 3.1 Compromised HMI Sends Malicious Commands to Devices -- 3.2 SCADA Firewall Fails and Critical Traffic Cannot Reach Devices -- 4 Analyzing Scenarios for a Railway System -- 4.1 Failure Scenario Analysis Tool -- 4.2 Case Study: Deploying SCADA Firewalls -- 4.3 Discussion -- 5 Related Work -- 6 Conclusion -- References -- Tamper Resistant Secure Digital Silo for Log Storage in Critical Infrastructures -- 1 Introduction -- 1.1 Contribution -- 1.2 Organization -- 2 Motivation -- 3 Background -- 3.1 Intel Software Guard Extensions (SGX) -- 3.2 Trusted Platform Module (TPM) -- 3.3 Enterprise Cryptographic Filesystem (eCryptfs) -- 3.4 Secure Block Device (SBD) -- 4 Design -- 5 Implementation and Evaluation -- 6 Conclusions and Future Work -- References.
Access Control and Availability Vulnerabilities in the ISO/IEC 61850 Substation Automation Protocol.

Sommario/riassunto

This book constitutes the post-conference proceedings of the 11th International Conference on Critical Information Infrastructures Security, CRITIS 2016, held in Paris, France, in October 2016. The 22 full papers and 8 short papers presented were carefully reviewed and selected from 58 submissions. They present the most recent innovations, trends, results, experiences and concerns in selected perspectives of critical information infrastructure protection covering the range from small-scale cyber-physical systems security via information infrastructures and their interaction with national and international infrastructures.

2. Record Nr. UNISALENTO991003219329707536

Autore	Aertsen, Jan A.
Titolo	Ende und Vollendung : eschatologische Perspektiven im Mittelalter ; mit einem Beitrag zur Geschichte des Thomas-Instituts der Universität zu Köln anlässlich des 50. Jahrestages der Institutsgründung / hrsg. von Jan A. Aertsen und Martin Pickave
Pubbl/distr/stampa	Berlin : de Gruyter, 2002
ISBN	3110172143
Descrizione fisica	xiii, 763 p. : ill. ; 25 cm
Collana	Miscellanea mediaevalia ; Bd. 29
Altri autori (Persone)	Pickavé, Martin
Lingua di pubblicazione	Tedesco
Formato	Materiale a stampa
Livello bibliografico	Monografia