1. Record Nr. UNISA996465371103316

Autore	Rass Stefan
Titolo	Cyber-Security in Critical Infrastructures [[electronic resource]] : A Game-Theoretic Approach / / by Stefan Rass, Stefan Schauer, Sandra König, Quanyan Zhu
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-46908-5
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (299 pages)
Collana	Advanced Sciences and Technologies for Security Applications, , 1613-5113
Disciplina	005.8
Soggetti	Computer security Game theory System safety Computer crimes Systems and Data Security Game Theory, Economics, Social and Behav. Sciences Security Science and Technology Game Theory Cybercrime
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Part 1. Introduction -- 1. Introduction -- 2. Critical Infrastructures -- 3. Mathematical Decision Making -- 4. Types of Games -- 5. Bounded Rationality -- Part II Security Games -- 6. Risk Management -- 7. Insurance -- 8. Patrolling and Surveillance Games. 9. Optimal Inspection Plans -- 10. Defense-in-Depth-Games -- 11. Cryptographic Games -- 12. Practicalities -- Acronyms -- Glossary -- List of Symbols -- Index.
Sommario/riassunto	This book presents a compendium of selected game- and decision-theoretic models to achieve and assess the security of critical infrastructures. Given contemporary reports on security incidents of various kinds, we can see a paradigm shift to attacks of an increasingly heterogeneous nature, combining different techniques into what we

know as an advanced persistent threat. Security precautions must match these diverse threat patterns in an equally diverse manner; in response, this book provides a wealth of techniques for protection and mitigation. Much traditional security research has a narrow focus on specific attack scenarios or applications, and strives to make an attack “practically impossible.” A more recent approach to security views it as a scenario in which the cost of an attack exceeds the potential reward. This does not rule out the possibility of an attack but minimizes its likelihood to the least possible risk. The book follows this economic definition of security, offering a management scientific view that seeks a balance between security investments and their resulting benefits. It focuses on optimization of resources in light of threats such as terrorism and advanced persistent threats. Drawing on the authors’ experience and inspired by real case studies, the book provides a systematic approach to critical infrastructure security and resilience. Presenting a mixture of theoretical work and practical success stories, the book is chiefly intended for students and practitioners seeking an introduction to game- and decision-theoretic techniques for security. The required mathematical concepts are self-contained, rigorously introduced, and illustrated by case studies. The book also provides software tools that help guide readers in the practical use of the scientific models and computational frameworks.