1. Record Nr. UNINA9910299348403321

| | |
|---|---|
| Titolo | Smart Micro-Grid Systems Security and Privacy / / edited by Anne V. D. M. Kayem, Stephen D. Wolthusen, Christoph Meinel |
| Pubbl/distr/stampa | Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018 |
| ISBN | 3-319-91427-8 |
| Edizione | [1st ed. 2018.] |
| Descrizione fisica | 1 online resource (174 pages) |
| Collana | Advances in Information Security, , 1568-2633 ; ; 71 |
| Disciplina | 621.319028558 |
| Soggetti | Data protection<br>Power electronics<br>Electrical engineering<br>Security<br>Power Electronics, Electrical Machines and Networks<br>Communications Engineering, Networks |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di bibliografia | Includes bibliographical references and index. |
| Nota di contenuto | 1 Power Systems: A Matter of Security and Privacy -- 2 A Review on Attacks and their Countermeasures in Power System State Estimation -- 3 An Anonymous Authentication Protocol for the Smart Grid -- 4 Attacks on Authentication and Authorization Models in Smart Grids -- 5 A Resilient Smart Micro-Grid Architecture for Resource Constrained Environments -- 6 The Design and Classification of Cheating Attacks on Power Marketing Schemes in Resource Constrained Smart Micro-Grids -- 7 Inferring Private User Behaviour Based on Information Leakage. |
| Sommario/riassunto | This book is centered on Smart grids and micro-grids, as a cost-effective method of ensuring fair and equitable access to power in urban areas. It also considers scenarios where deploying smart grids can be both cost-prohibitively expensive and logistically challenging. Deploying smart microgrids instead, offers a reliable power solution but, as is the case in smart grids, a key issue is guaranteeing usability, trust, and reliability while protecting against energy theft. This book considers aspects such as state estimation, capacity planning, demand |

forecasting, price signals, and demand management with respect to energy theft. Straight-forward approaches to provoking energy theft on smart grids and micro-grids include mis-recordings power consumption/generation information and exposures of personally identifiable information or sensitive information. Attack models based on mis-recorded generation and/or consumption data and exposure of personally identifiable information, are also studied. In each case, countermeasures are proposed to circumvent the power theft attacks raised. Researchers in Smart Micro-grids security, cyber-physical systems, and critical infrastructure will want to purchase this book as a reference. Professionals, Researchers, Academics and students working in security general and Security of Critical Infrastructure, Privacy, and Data Sharing will also want to purchase this book as a reference.