1. Record Nr. UNINA9910299357803321

Titolo	Versatile Cybersecurity / / edited by Mauro Conti, Gaurav Somani, Radha Poovendran
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
ISBN	3-319-97643-5
Edizione	[1st ed. 2018.]
Descrizione fisica	1 online resource (295 pages)
Collana	Advances in Information Security, , 1568-2633 ; ; 72
Disciplina	005.8
Soggetti	Data protection Computer communication systems Computer security Security Computer Communication Networks Systems and Data Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	1 An Android-based Covert Channel Framework on Wearables Using Status Bar Notifications -- 2 Insider Threat Detection: Machine Learning Way -- 3 Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions -- 4 Protection Against Semantic Social Engineering Attacks -- 5 Cryptographic Program Obfuscation: Practical Solutions and Application-Driven Models -- 6 Botnet-Based Attacks and Defense Mechanisms -- 7 Catastrophic Cyber-Physical Malware -- 8 Cross-VM Attacks: Attack Taxonomy, Defense Mechanisms, and New Directions.
Sommario/riassunto	Cyber security research is one of the important areas in the computer science domain which also plays a major role in the life of almost every individual, enterprise, society and country, which this book illustrates. A large number of advanced security books focus on either cryptography or system security which covers both information and network security. However, there is hardly any books available for advanced-level students and research scholars in security research to systematically study how the major attacks are studied, modeled,

planned and combated by the community. This book aims to fill this gap. This book provides focused content related to specific attacks or attack families. These dedicated discussions in the form of individual chapters covers the application or area specific aspects, while discussing the placement of defense solutions to combat the attacks. It includes eight high quality chapters from established security research groups worldwide, which address important attacks from theoretical (modeling) as well as practical aspects. Each chapter brings together comprehensive and structured information on an attack or an attack family. The authors present crisp detailing on the state of the art with quality illustration of defense mechanisms and open research problems. This book also covers various important attacks families such as insider threats, semantics social engineering attacks, distributed denial of service attacks, botnet based attacks, cyber physical malware based attacks, cross-vm attacks, and IoT covert channel attacks. This book will serve the interests of cyber security enthusiasts, undergraduates, post-graduates, researchers and professionals working in this field. .