New Threats And Countermeasures In Digital Crime And Cyber Terrorism Advances In Digital Crime Forensics And Cyber Terrorism

Provides research on the social and human aspects of information security. Presents the latest trends, issues, and findings in the field.
This 24-hour free course introduced online security: how to recognise threats and take steps to reduce the chances that they will occur.
FOSAD has been one of the foremost educational events established with the goal of disseminating knowledge in the critical area of security in computer systems and networks. Over the years, both the summer school and the book series have represented a reference point for graduate students and young researchers from academia and industry, interested to approach the field, investigate open problems, and follow priority lines of research. This book presents thoroughly revised versions of four tutorial lectures given by leading researchers during three International Schools on Foundations of Security Analysis and Design, FOSAD, held in Bertinoro, Italy, in September 2014, 2015 and 2016. The topics covered in this book include zero-knowledge proof systems, JavaScript sandboxing, assessment of privacy, and distributed authorization.
Through expanded intelligence, the use of robotics has fundamentally transformed a variety of fields, including manufacturing, aerospace, medicine, social services, and agriculture. Continued research on robotic design is critical to solving various dynamic obstacles individuals, enterprises, and humanity at large face on a daily basis. Robotic Systems: Concepts, Methodologies, Tools, and Applications is a vital reference source that delves into the current issues, methodologies, and trends relating to advanced robotic technology in the modern world. Highlighting a range of topics such as mechatronics, cybernetics, and human-computer interaction, this multi-volume book is ideally designed for robotics engineers, mechanical engineers, robotics technicians, operators, software engineers, designers, programmers, industry professionals, researchers, students, academicians, and computer practitioners seeking current research on developing innovative ideas for intelligent and autonomous robotics systems.
The communication field is evolving rapidly in order to keep up with society’s demands. As such, it becomes imperative to research and report recent advancements in computational intelligence as it applies to communication networks. The Handbook of Research on Recent Developments in Intelligent Communication Application is a pivotal reference source for the latest developments on emerging data communication applications. Featuring extensive coverage across a range of relevant perspectives and topics, such as satellite communication, cognitive radio networks, and wireless sensor networks, this book is ideally designed for engineers, professionals, practitioners, upper-level students, and academics seeking current information on emerging communication networking trends.
The LNCS series reports state-of-the-art results in computer science research, development, and education, at a high level and in both printed and electronic form. Enjoying tight cooperation with the R&D community, with numerous individuals, as well as with prestigious organizations and societies, LNCS has grown into the most comprehensive computer science research forum available. The Scope of LNCS, including its subseries LNAI and LNBI, spans the whole range of computer science and information technology including interdisciplinary topics in a variety of application fields. In parallel to the printed book, each new volume is published electronically in LNCS Online.
New Threats and Countermeasures in Digital Crime and Cyber TerrorismIGI Global
Technological advances, although beneficial and progressive, can lead to vulnerabilities in system networks and security. While researchers attempt to find solutions, negative uses of technology continue to create new security threats to users. New Threats and Countermeasures in Digital Crime and Cyber Terrorism brings together research-based chapters and case studies on security techniques and current methods being used to identify and overcome technological vulnerabilities with an emphasis on security issues in mobile computing and online activities. This book is an essential reference source for researchers, university academics, computing professionals, and upper-level students interested in the techniques, laws, and training initiatives currently being implemented and adapted for secure computing.
"An extensive collection of significant documents covering all major and minor issues and events regarding terrorism. Government reports, executive orders, speeches, court proceedings, and position papers are presented in full text reprint"--Oceana Website.
A suggested approach to the policy issue of what and how much should be done by the Government of Israel to counter the objective threat of Palestinian terrorism. Palestinian terrorism is defined as Palestinian acts of low-level violence carried out for a political purpose, with the intent of inflicting casualties and damage as well as inducing fear and rage in Israeli society, and by so doing to incite Israel to react. After a historical analysis of Palestinian violence and Israeli countermeasures, the study focuses on current perceptions and observations. Terrorism is perceived by Israeli society as a major threat, both as a threat to the individual and as damaging to the national image. The perception of terrorism, however, is out of proportion to the share of terrorism in causing casualties, the reasons for which are given. The author suggests that Israel reduce the discrepancy in resource allocation among all casualty-preventing programs (say, preventing car accidents as well as countering terrorism); ameliorate society's perception of the subjective danger of terrorism; and, in general, to not react as expected to terrorist provocations. The study was prepared as a dissertation for the RAND Graduate Institute.
During public health emergencies such as terrorist attacks or influenza outbreaks, the public health system's ability to save lives could depend on dispensing medical countermeasures such as antibiotics, antiviral medications, and vaccines to a large number of people in a short amount of time. The IOM's Forum on Medical and Public Health Preparedness for Catastrophic Events held a workshop on November 18, 2009, to provide an overview of current threats, recent progress made in the public health system for distributing and dispensing countermeasures, and remaining vulnerabilities.
This book constitutes revised selected papers from the 6th International Workshop on Critical Information Infrastructure Security, CRITIS 2011, held in Lucerne, Switzerland, in September 2011. The 16 full papers and 6 short papers presented in this volume were carefully reviewed and selected from 38 submissions. They deal with all areas of critical infrastructure protection research.
Cyber attacks are rapidly becoming one of the most prevalent issues in the world. As cyber crime continues to escalate, it is imperative to explore new approaches and technologies that help ensure the security of the online community. The Handbook of Research on Threat Detection and Countermeasures in Network Security presents the latest methodologies and trends in detecting and preventing network threats. Investigating the potential of current and emerging security technologies, this publication is an all-inclusive reference source for

academicians, researchers, students, professionals, practitioners, network analysts, and technology specialists interested in the simulation and application of computer network protection.

This book gathers recent research works in emerging Artificial Intelligence (AI) methods for the convergence of communication, caching, control, and computing resources in cloud-based Internet of Vehicles (IoV) infrastructures. In this context, the book's major subjects cover the analysis and the development of AI-powered mechanisms in future IoV applications and architectures. It addresses the major new technological developments in the field and reflects current research trends and industry needs. It comprises a good balance between theoretical and practical issues, covering case studies, experience and evaluation reports, and best practices in utilizing AI applications in IoV networks. It also provides technical/scientific information about various aspects of AI technologies, ranging from basic concepts to research-grade material, including future directions. This book is intended for researchers, practitioners, engineers, and scientists involved in designing and developing protocols and AI applications and services for IoV-related devices.