2013 Ieee Papers On Ethical Hacking

Getting the books **2013 Ieee Papers On Ethical Hacking** now is not type of inspiring means. You could not unaided going as soon as ebook accrual or library or borrowing from your contacts to approach them. This is an no question easy means to specifically acquire guide by on-line. This online pronouncement 2013 Ieee Papers On Ethical Hacking can be one of the options to accompany you following having new time.

It will not waste your time. say you will me, the e-book will unquestionably announce you supplementary event to read. Just invest tiny time to admission this on-line message **2013 Ieee Papers On Ethical Hacking** as capably as review them wherever you are now.

Certified Ethical Hacker (CEH) Cert Guide - Michael Gregg 2013-08-30
Accompanying CD-ROM contains: Pearson IT Certification Practice Test Engine, with two practice exams and access to a large library of exam-realistic questions; memory tables, lists, and other resources, all in searchable PDF format.
Information and Communication Technologies of Ecuador (TIC.EC) - Miguel Botto-Tobar 2018-10-17
This book constitutes the proceedings of the 6th Conference on Information Technologies and Communication of Ecuador "TIC-EC", held in Riobamba City from November 21 to 23, 2018, and organized by Universidad Nacional del Chimborazo (UNACH) and its Engineering School, and the Ecuadorian Corporation for the Development of Research and Academia (CEDIA). Considered as one of the most important ICT conferences in Ecuador, it brought together international scholars and practitioners to discuss the development, issues and projections of the use of information and communication technologies in multiple fields of application. Presenting high-quality, peer-reviewed papers, the book discusses the following topics: • Communication networks • Software engineering • Computer sciences • Architecture • Intelligent territory management • IT management • Web technologies • ICT in education • Engineering, industry, and construction with ICT support • Entrepreneurship and innovation at the Academy: a business perspective The authors would like to express their sincere gratitude to the invited speakers for their inspirational talks, to the authors for submitting their work to this conference, and the reviewers for sharing their experience during the selection process.
Emerging Technologies in Computing - Mahdi H. Miraz 2018-07-20
This book constitutes the refereed conference proceedings of the First International Conference on Emerging Technologies in Computing, iCEtiC 2018, held in London, UK, in August 2018. The 26 revised full papers were reviewed and selected from more than 59 submissions and are organized in topical sections covering Cloud, IoT and distributed computing, software engineering, communications engineering and vehicular technology, AI, expert systems and big data analytics, Web information systems and applications, security, database system, economics and business engineering, mLearning and eLearning.
Methods, Implementation, and Application of Cyber Security Intelligence and Analytics - Om Prakash, Jena 2022-06-17
Cyber security is a key focus in the modern world as more private information is stored and saved online. In order to ensure vital information is protected from various cyber threats, it is essential to develop a thorough understanding of technologies that can address cyber security challenges. Artificial intelligence has been recognized as an important technology that can be employed successfully in the cyber security sector. Due to this, further study on the potential uses of artificial intelligence is required. Methods, Implementation, and Application of Cyber Security Intelligence and Analytics discusses critical artificial intelligence technologies that are utilized in cyber security and considers various cyber security issues and their optimal solutions supported by artificial intelligence. Covering a range of topics such as malware, smart grid, data breachers, and machine learning, this major reference work is ideal for security analysts, cyber security specialists, data analysts, security professionals, computer scientists, government officials, researchers, scholars, academicians, practitioners, instructors, and students.
Cyber-Assurance for the Internet of Things - Tyson T. Brooks 2017-01-04
Presents an Cyber-Assurance approach to the Internet of Things (IoT) This book discusses the cyber-assurance needs of the IoT environment, highlighting key information assurance (IA) IoT issues and identifying the associated security implications. Through contributions from cyber-assurance, IA, information security and IoT industry practitioners and experts, the text covers fundamental and advanced concepts necessary to grasp current IA issues, challenges, and solutions for the IoT. The future trends in IoT infrastructures, architectures and applications are also examined. Other topics discussed include the IA protection of IoT systems and information being stored, processed or transmitted from unauthorized access or modification of machine-2-machine (M2M) devices, radio-frequency identification (RFID) networks, wireless sensor networks, smart grids, and supervisory control and data acquisition (SCADA) systems. The book also discusses IA measures necessary to detect, protect, and defend IoT information and networks/systems to ensure their availability, integrity, authentication, confidentially, and non-repudiation. Discusses current research and emerging trends in IA theory, applications, architecture and information security in the IoT based on theoretical aspects and studies of practical applications Aids readers in understanding how to design and build cyber-assurance into the IoT Exposes engineers and designers to new strategies and emerging standards, and promotes active development of cyber-assurance Covers challenging issues as well as potential solutions, encouraging discussion and debate amongst those in the field Cyber-Assurance for the Internet of Things is written for researchers and professionals working in the field of wireless technologies, information security architecture, and security system design. This book will also serve as a reference for professors and students involved in IA and IoT networking. Tyson T. Brooks is an Adjunct Professor in the School of Information Studies at Syracuse University; he also works with the Center for Information and Systems Assurance and Trust (CISAT) at Syracuse University, and is an information security technologist and science-practitioner. Dr. Brooks is the founder/Editor-in-Chief of the International Journal of Internet of Things and Cyber-Assurance, an associate editor for the Journal of Enterprise Architecture, the International Journal of Cloud Computing and Services Science, and the International Journal of Information and Network Security.
Selected Readings in Cybersecurity - Young B. Choi 2018-11-16
This collection of papers highlights the current state of the art of cybersecurity. It is divided into five major sections: humans and information security; security systems design and development; security systems management and testing; applications of information security technologies; and outstanding cybersecurity technology development trends. This book will mainly appeal to practitioners in the cybersecurity industry and college faculty and students in the disciplines of cybersecurity, information systems, information technology, and computer science.
Research Anthology on Advancements in Cybersecurity Education - Management Association, Information Resources 2021-08-27
Modern society has become dependent on technology, allowing personal information to be input and used across a variety of personal and professional systems. From banking to medical records to e-commerce, sensitive data has never before been at such a high risk of misuse. As such, organizations now have a greater responsibility than ever to ensure that their stakeholder data is secured, leading to the increased

need for cybersecurity specialists and the development of more secure software and systems. To avoid issues such as hacking and create a safer online space, cybersecurity education is vital and not only for those seeking to make a career out of cybersecurity, but also for the general public who must become more aware of the information they are sharing and how they are using it. It is crucial people learn about cybersecurity in a comprehensive and accessible way in order to use the skills to better protect all data. The Research Anthology on Advancements in Cybersecurity Education discusses innovative concepts, theories, and developments for not only teaching cybersecurity, but also for driving awareness of efforts that can be achieved to further secure sensitive data. Providing information on a range of topics from cybersecurity education requirements, cyberspace security talents training systems, and insider threats, it is ideal for educators, IT developers, education professionals, education administrators, researchers, security analysts, systems engineers, software security engineers, security professionals, policymakers, and students.

The Cyber Security Handbook - Prepare for, respond to and recover from cyber attacks - Alan Calder 2020-12-10

This book is a comprehensive cyber security implementation manual which gives practical guidance on the individual activities identified in the IT Governance Cyber Resilience Framework (CRF) that can help organisations become cyber resilient and combat the cyber threat landscape. Start your cyber security journey and buy this book today!

Crowd Assisted Networking and Computing - Al-Sakib Khan Pathan 2018-09-03

Crowd computing, crowdsourcing, crowd-associated network (CrAN), crowd-assisted sensing are some examples of crowd-based concepts that harness the power of people on the web or connected via web-like infrastructure to do tasks that are often difficult for individual users or computers to do alone. This creates many challenging issues like assessing reliability and correctness of crowd generated information, delivery of data and information via crowd, middleware for supporting crowdsourcing and crowd computing tasks, crowd associated networking and its security, Quality of Information (QoI) issues, etc. This book compiles the latest advances in the relevant fields.

Security and Privacy in the Internet of Things - Ali Ismail Awad 2021-12-29

SECURITY AND PRIVACY IN THE INTERNET OF THINGS Provides the authoritative and up-to-date information required for securing IoT architecture and applications The vast amount of data generated by the Internet of Things (IoT) has made information and cyber security vital for not only personal privacy, but also for the sustainability of the IoT itself. Security and Privacy in the Internet of Things brings together high-quality research on IoT security models, architectures, techniques, and application domains. This concise yet comprehensive volume explores state-of-the-art mitigations in IoT security while addressing important security and privacy challenges across different IoT layers. The book provides timely coverage of IoT architecture, security technologies and mechanisms, and applications. The authors outline emerging trends in IoT security and privacy with a focus on areas such as smart environments and e-health. Topics include authentication and access control, attack detection and prevention, securing IoT through traffic modeling, human aspects in IoT security, and IoT hardware security. Presenting the current body of knowledge in a single volume, Security and Privacy in the Internet of Things: Discusses a broad range of IoT attacks and defense mechanisms Examines IoT security and privacy protocols and approaches Covers both the logical and physical security of IoT devices Addresses IoT security through network traffic modeling Describes privacy preserving techniques in smart cities Explores current threat and vulnerability analyses Security and Privacy in the Internet of Things: Architectures, Techniques, and Applications is essential reading for researchers, industry practitioners, and students involved in IoT security development and IoT systems deployment.

Computational Intelligent Security in Wireless Communications - Suhel Ahmed Khan 2022-09-21

Wireless network security research is multidisciplinary in nature, including data analysis, economics, mathematics, forensics, information technology, and computer science. This text covers cutting-edge research in computational intelligence systems from diverse fields on the complex subject of wireless communication security. It discusses important topics including computational intelligence in wireless network and communications, artificial intelligence and wireless communication security, security risk scenarios in communications, security/resilience metrics and their measurements, data analytics of cyber-crimes, modeling of wireless communication security risks, advances in cyber threats and computer crimes, adaptive and learning techniques for secure estimation and control, decision support systems, fault tolerance and diagnosis, cloud forensics and information systems, and intelligent information retrieval. The book- Discusses computational algorithms for system modeling and optimization in security perspective. Focuses on error prediction and fault diagnosis through intelligent information retrieval via wireless technologies. Explores a group of practical research problems where security experts can help develop new data-driven methodologies. Covers application on artificial intelligence and wireless communication security risk perspective The text is primarily written for senior undergraduate, graduate students, and researchers in the fields of electrical engineering, electronics and communication engineering, and computer engineering. The text comprehensively discusses wide range of wireless communication techniques with emerging computational intelligent trends, to help readers understand the role of wireless technologies in applications touching various spheres of human life with the help of hesitant fuzzy sets based computational modeling. It will be a valuable resource for senior undergraduate, graduate students, and researchers in the fields of electrical engineering, electronics and communication engineering, and computer engineering.

Information Security Technologies for Controlling Pandemics - Hamid Jahankhani 2021-07-29

The year 2020 and the COVID-19 pandemic marked a huge change globally, both in working and home environments. They posed major challenges for organisations around the world, which were forced to use technological tools to help employees work remotely, while in self-isolation and/or total lockdown. Though the positive outcomes of using these technologies are clear, doing so also comes with its fair share of potential issues, including risks regarding data and its use, such as privacy, transparency, exploitation and ownership. COVID-19 also led to a certain amount of paranoia, and the widespread uncertainty and fear of change represented a golden opportunity for threat actors. This book discusses and explains innovative technologies such as blockchain and methods to defend from Advanced Persistent Threats (APTs), some of the key legal and ethical data challenges to data privacy and security presented by the COVID-19 pandemic, and their potential consequences. It then turns to improved decision making in cyber security, also known as cyber situational awareness, by analysing security events and comparing data mining techniques, specifically classification techniques, when applied to cyber security data. In addition, the book illustrates the importance of cyber security, particularly information integrity and surveillance, in dealing with an on-going, infectious crisis. Aspects addressed range from the spread of misinformation, which can lead people to actively work against measures designed to ensure public safety and minimise the spread of the virus, to concerns over the approaches taken to monitor, track, trace and isolate infectious cases through the use of technology. In closing, the book considers the legal, social and ethical cyber and information security implications of the pandemic and responses to it from the perspectives of confidentiality, integrity and availability.

Hack the world - Ethical Hacking - Abhijeet Prakash

Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019) - Pradeep Kumar Singh 2020-04-27

This book features selected research papers presented at the First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019), organized by Northwest Group of Institutions, Punjab, India, Southern Federal University, Russia, and IAC Educational Trust, India along with KEC, Ghaziabad and

ITS, College Ghaziabad as an academic partner and held on 12-13 October 2019. It includes innovative work from researchers, leading innovators and professionals in the area of communication and network technologies, advanced computing technologies, data analytics and intelligent learning, the latest electrical and electronics trends, and security and privacy issues.

Professional Penetration Testing - Thomas Wilhelm 2013-06-27

Professional Penetration Testing walks you through the entire process of setting up and running a pen test lab. Penetration testing—the act of testing a computer network to find security vulnerabilities before they are maliciously exploited—is a crucial component of information security in any organization. With this book, you will find out how to turn hacking skills into a professional career. Chapters cover planning, metrics, and methodologies; the details of running a pen test, including identifying and verifying vulnerabilities; and archiving, reporting and management practices. Author Thomas Wilhelm has delivered penetration testing training to countless security professionals, and now through the pages of this book you can benefit from his years of experience as a professional penetration tester and educator. After reading this book, you will be able to create a personal penetration test lab that can deal with real-world vulnerability scenarios. All disc-based content for this title is now available on the Web. Find out how to turn hacking and pen testing skills into a professional career Understand how to conduct controlled attacks on a network through real-world examples of vulnerable and exploitable servers Master project management skills necessary for running a formal penetration test and setting up a professional ethical hacking business Discover metrics and reporting methodologies that provide experience crucial to a professional penetration tester

The "Essence" of Network Security: An End-to-End Panorama - Mohuya Chakraborty 2020-11-24

This edited book provides an optimal portrayal of the principles and applications related to network security. The book is thematically divided into five segments: Part A describes the introductory issues related to network security with some concepts of cutting-edge technologies; Part B builds from there and exposes the readers to the digital, cloud and IoT forensics; Part C presents readers with blockchain and cryptography techniques; Part D deals with the role of AI and machine learning in the context of network security. And lastly, Part E is written on different security networking methodologies. This is a great book on network security, which has lucid and well-planned chapters. All the latest security technologies are thoroughly explained with upcoming research issues. Details on Internet architecture, security needs, encryption, cryptography along with the usages of machine learning and artificial intelligence for network security are presented in a single cover. The broad-ranging text/reference comprehensively surveys network security concepts, methods, and practices and covers network security policies and goals in an integrated manner. It is an essential security resource for practitioners in networks and professionals who develop and maintain secure computer networks.

The Cloud Security Ecosystem - Ryan Ko 2015-06-01

Drawing upon the expertise of world-renowned researchers and experts, The Cloud Security Ecosystem comprehensively discusses a range of cloud security topics from multi-disciplinary and international perspectives, aligning technical security implementations with the most recent developments in business, legal, and international environments. The book holistically discusses key research and policy advances in cloud security - putting technical and management issues together with an in-depth treaties on a multi-disciplinary and international subject. The book features contributions from key thought leaders and top researchers in the technical, legal, and business and management aspects of cloud security. The authors present the leading edge of cloud security research, covering the relationships between differing disciplines and discussing implementation and legal challenges in planning, executing, and using cloud security. Presents the most current and leading-edge research on cloud security from a multi-disciplinary standpoint, featuring a panel of top experts in the field Focuses on the technical, legal, and business management issues involved in implementing effective cloud security, including case examples Covers key technical topics, including cloud trust protocols, cryptographic deployment and key management, mobile devices and BYOD security management, auditability and accountability, emergency and incident response, as well as cloud forensics Includes coverage of management and legal issues such as cloud data governance, mitigation and liability of international cloud deployment, legal boundaries, risk management, cloud information security management plans, economics of cloud security, and standardization efforts

Foundations of Information Ethics - John T. F. Burgess 2019-07-03

Foreword by Robert Hauptman As discussions about the roles played by information in economic, political, and social arenas continue to evolve, the need for an intellectual primer on information ethics that also functions as a solid working casebook for LIS students and professionals has never been more urgent. This text, written by a stellar group of ethics scholars and contributors from around the globe, expertly fills that need. Organized into twelve chapters, making it ideal for use by instructors, this volume from editors Burgess and Knox thoroughly covers principles and concepts in information ethics, as well as the history of ethics in the information professions; examines human rights, information access, privacy, discourse, intellectual property, censorship, data and cybersecurity ethics, intercultural information ethics, and global digital citizenship and responsibility; synthesizes the philosophical underpinnings of these key subjects with abundant primary source material to provide historical context along with timely and relevant case studies; features contributions from John M. Budd, Paul T. Jaeger, Rachel Fischer, Margaret Zimmerman, Kathrine A. Henderson, Peter Darch, Michael Zimmer, and Masooda Bashir, among others; and offers a special concluding chapter by Amelia Gibson that explores emerging issues in information ethics, including discussions ranging from the ethics of social media and social movements to AI decision making. This important survey will be a key text for LIS students and an essential reference work for practitioners.

Hands-On Ethical Hacking and Network Defense - Michael T. Simpson 2010-03-17

Hands-On Ethical Hacking and Network Defense, Second Edition provides an in-depth understanding of how to effectively protect computer networks. This book describes the tools and penetration testing methodologies used by ethical hackers and provides a thorough discussion of what and who an ethical hacker is and how important they are in protecting corporate and government data from cyber attacks. Readers are provided with updated computer security resources that describe new vulnerabilities and innovative methods to protect networks. Also included is a thorough update of federal and state computer crime laws, as well as changes in penalties for illegal computer hacking. With cyber-terrorism and corporate espionage threatening the fiber of our world, the need for trained network security professionals continues to grow. Hands-On Ethical Hacking and Network Defense, Second Edition provides a structured knowledge base to prepare readers to be security professionals who understand how to protect a network by using the skills and tools of an ethical hacker. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Emerging Methods in Predictive Analytics: Risk Management and Decision-Making - Hsu, William H. 2014-01-31

Decision making tools are essential for the successful outcome of any organization. Recent advances in predictive analytics have aided in identifying particular points of leverage where critical decisions can be made. Emerging Methods in Predictive Analytics: Risk Management and Decision Making provides an interdisciplinary approach to predictive analytics; bringing together the fields of business, statistics, and information technology for effective decision making. Managers, business professionals, and decision makers in diverse fields will find the applications and cases presented in this text essential in providing new avenues for risk assessment, management, and predicting the future outcomes of their decisions.

Advanced Information Systems Engineering Workshops -

John Krogstie 2016-06-06
This book constitutes the thoroughly refereed proceedings of five international workshops held in Ljubljana, Slovenia, in conjunction with the 28th International Conference on Advanced Information Systems Engineering, CAiSE 2016, in June 2016. The 16 full and 9 short papers were carefully selected from 51 submissions. The associated workshops were the Third International Workshop on Advances in Services DEsign based on the Notion of CApabiliy (ASDENCA) co-arranged with the First International Workshop on Business Model Dynamics and Information Systems Engineering (BumDISE), the Fourth International Workshop on Cognitive Aspects of Information Systems Engineering (COGNISE), the First International Workshop on Energy-awareness and Big Data Management in Information Systems (EnBIS), the Second International Workshop on Enterprise Modeling (EM), and the Sixth International Workshop on Information Systems Security Engineering (WISSE).

Security and Privacy in Cyberspace - Omprakash Kaiwartya 2022
This book highlights the literature and the practical aspects to understand cybersecurity and privacy in various networks and communication devices. It provides details of emerging technologies on various networks by protecting the privacy and security of cyberspace. This book presents state-of-the-art advances in the field of cryptography and network security, cybersecurity and privacy, providing a good reference for professionals and researchers.

Proceedings of International Ethical Hacking Conference 2019 - Mohuya Chakraborty 2019-11-29
This book gathers the peer-reviewed proceedings of the International Ethical Hacking Conference, eHaCON 2019, the second international conference of its kind, which was held in Kolkata, India, in August 2019. Bringing together the most outstanding research papers presented at the conference, the book shares new findings on computer network attacks and defenses, commercial security solutions, and hands-on, real-world security lessons learned. The respective sections include network security, ethical hacking, cryptography, digital forensics, cloud security, information security, mobile communications security, and cyber security.

The Ethics of Cybersecurity - Markus Christen 2020-02-10
This open access book provides the first comprehensive collection of papers that provide an integrative view on cybersecurity. It discusses theories, problems and solutions on the relevant ethical issues involved. This work is sorely needed in a world where cybersecurity has become indispensable to protect trust and confidence in the digital infrastructure whilst respecting fundamental values like equality, fairness, freedom, or privacy. The book has a strong practical focus as it includes case studies outlining ethical issues in cybersecurity and presenting guidelines and other measures to tackle those issues. It is thus not only relevant for academics but also for practitioners in cybersecurity such as providers of security software, governmental CERTs or Chief Security Officers in companies.

The Changing Scope of Technoethics in Contemporary Society - Luppicini, Rocci 2018-04-13
In the modern era each new innovation poses its own special ethical dilemma. How can human society adapt to these new forms of expression, commerce, government, citizenship, and learning while holding onto its ethical and moral principles? The Changing Scope of Technoethics in Contemporary Society is a critical scholarly resource that examines the existing intellectual platform within the field of technoethics. Featuring coverage on a broad range of topics such as ethical perspectives on internet safety, technoscience, and ethical hacking communication, this book is geared towards academicians, researchers, and students seeking current research on domains of technoethics.

Combating Security Breaches and Criminal Activity in the Digital Sphere - Geetha, S. 2016-06-09
With the rapid advancement in technology, a myriad of new threats have emerged in online environments. The broad spectrum of these digital risks requires new and innovative methods for protection against cybercrimes. Combating Security Breaches and Criminal Activity in the Digital Sphere is a pivotal reference source for the latest scholarly research on current trends in cyber forensic investigations, focusing on advanced techniques for protecting information security and preventing potential exploitation for online users. Featuring law enforcement perspectives, theoretical foundations, and forensic methods, this book is ideally designed for policy makers, analysts, researchers, technology developers, and upper-level students.

ICCWS 2019 14th International Conference on Cyber Warfare and Security - Noëlle van der Waag-Cowling 2019-02-28

Constructing an Ethical Hacking Knowledge Base for Threat Awareness and Prevention - Dhavale, Sunita Vikrant 2018-12-14
In recent decades there has been incredible growth in the use of various internet applications by individuals and organizations who store sensitive information online on different servers. This greater reliance of organizations and individuals on internet technologies and applications increases the threat space and poses several challenges for implementing and maintaining cybersecurity practices. Constructing an Ethical Hacking Knowledge Base for Threat Awareness and Prevention provides innovative insights into how an ethical hacking knowledge base can be used for testing and improving the network and system security posture of an organization. It is critical for each individual and institute to learn hacking tools and techniques that are used by dangerous hackers in tandem with forming a team of ethical hacking professionals to test their systems effectively. Highlighting topics including cyber operations, server security, and network statistics, this publication is designed for technical experts, students, academicians, government officials, and industry professionals.

HCI Challenges and Privacy Preservation in Big Data Security - Lopez, Daphne 2017-08-10
Privacy protection within large databases can be a challenge. By examining the current problems and challenges this domain is facing, more efficient strategies can be established to safeguard personal information against invasive pressures. HCI Challenges and Privacy Preservation in Big Data Security is an informative scholarly publication that discusses how human-computer interaction impacts privacy and security in almost all sectors of modern life. Featuring relevant topics such as large scale security data, threat detection, big data encryption, and identity management, this reference source is ideal for academicians, researchers, advanced-level students, and engineers that are interested in staying current on the advancements and drawbacks of human-computer interaction within the world of big data.

Wireless Hacking 101 - Karina Astudillo 2017-10-10
Wireless Hacking 101 - How to hack wireless networks easily! This book is perfect for computer enthusiasts that want to gain expertise in the interesting world of ethical hacking and that wish to start conducting wireless pentesting. Inside you will find step-by-step instructions about how to exploit WiFi networks using the tools within the known Kali Linux distro as the famous aircrack-ng suite. Topics covered: •Introduction to WiFi Hacking •What is Wardriving •WiFi Hacking Methodology •WiFi Mapping •Attacks to WiFi clients and networks •Defeating MAC control •Attacks to WEP, WPA, and WPA2 •Attacks to WPS •Creating Rogue AP's •MITM attacks to WiFi clients and data capture •Defeating WiFi clients and evading SSL encryption •Kidnapping sessions from WiFi clients •Defensive mechanisms

Privacy and Identity Management - Michael Friedewald 2021-05-02
This book contains selected papers presented at the 15th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School on Privacy and Identity Management, held in Maribor, Slovenia, in September 2020.* The 13 full papers included in this volume were carefully reviewed and selected from 21 submissions. Also included is a summary paper of a tutorial. As in previous years, one of the goals of the IFIP Summer School was to encourage the publication of thorough research papers by students and emerging scholars. The papers combine interdisciplinary approaches to bring together a host of perspectives, such as technical, legal, regulatory, socio-economic, social or societal, political, ethical, anthropological, philosophical, or psychological perspectives. *The summer school was held virtually.

Proceedings of International Ethical Hacking Conference 2018 - Mohuya Chakraborty 2018-10-04
This book discusses the implications of new technologies for a secured society. As such, it reflects the main

focus of the International Conference on Ethical Hacking, eHaCon 2018, which is essentially in evaluating the security of computer systems using penetration testing techniques. Showcasing the most outstanding research papers presented at the conference, the book shares new findings on computer network attacks and defenses, commercial security solutions, and hands-on, real-world security experience. The respective sections include network security, ethical hacking, cryptography, digital forensics, cloud security, information security, mobile communications security, and cyber security.
2019 Second International Conference on Latest Trends in Electrical Engineering and Computing Technologies (INTELLECT) - 2019

Security Standardisation Research - Thyla van der Merwe 2020-11-24
This book constitutes the refereed proceedings of the 6th International Conference on Security Standardisation Research, SSR 2020, held in London, UK, in November 2020.* The papers cover a range of topics in the field of security standardisation research, including cryptographic evaluation, standards development, analysis with formal methods, potential future areas of standardisation, and improving existing standards. * The conference was held virtually due to the COVID-19 pandemic.
Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention - Conteh, Nabie Y. 2021-06-25
As personal data continues to be shared and used in all aspects of society, the protection of this information has become paramount. While cybersecurity should protect individuals from cyber-threats, it also should be eliminating any and all vulnerabilities. The use of hacking to prevent cybercrime and contribute new countermeasures towards protecting computers, servers, networks, web applications, mobile devices, and stored data from black hat attackers who have malicious intent, as well as to stop against unauthorized access instead of using hacking in the traditional sense to launch attacks on these devices, can contribute emerging and advanced solutions against cybercrime. Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention is a comprehensive text that discusses and defines ethical hacking, including the skills and concept of ethical hacking, and studies the countermeasures to prevent and stop cybercrimes, cyberterrorism, cybertheft, identity theft, and computer-related crimes. It broadens the understanding of cybersecurity by providing the necessary tools and skills to combat cybercrime. Some specific topics include top cyber investigation trends, data security of consumer devices, phases of hacking attacks, and stenography for secure image transmission. This book is relevant for ethical hackers, cybersecurity analysts, computer forensic experts, government officials, practitioners, researchers, academicians, and students interested in the latest techniques for preventing and combatting cybercrime.
White Hat Hacking - Jonathan Smith 2014-12-15
With every new technological development comes the need for specialists who know how to make products strong, secure, and private. White hat hacking is one of the hottest jobs in tech today?find out how to make it your career.
Smart Cities Cybersecurity and Privacy - Danda B. Rawat 2018-12-04
Smart Cities Cybersecurity and Privacy examines the latest research developments and their outcomes for safe, secure, and trusting smart cities residents. Smart cities improve the quality of life of citizens in their energy and water usage, healthcare, environmental impact, transportation needs, and many other critical city services. Recent advances in hardware and software, have fueled the rapid growth and deployment of ubiquitous connectivity between a city's physical and cyber components. This connectivity however also opens up many security vulnerabilities that must be mitigated. Smart Cities Cybersecurity and Privacy helps researchers, engineers, and city planners develop adaptive, robust, scalable, and reliable security and privacy smart city applications that can mitigate the negative implications associated with cyber-attacks and potential privacy invasion. It provides insights into networking and security architectures, designs, and models for the secure operation of smart city applications. Consolidates in one place state-of-the-art academic and industry research Provides a holistic and systematic framework for design, evaluating, and deploying the latest security solutions for smart cities Improves understanding and collaboration among all smart city stakeholders to develop more secure smart city architectures
Wireless and Mobile Device Security - Jim Doherty 2021-03-31
Written by an industry expert, Wireless and Mobile Device Security explores the evolution of wired networks to wireless networking and its impact on the corporate world.
Ethical Hacking - Alana Maurushat 2019-04-09
How will governments and courts protect civil liberties in this new era of hacktivism? Ethical Hacking discusses the attendant moral and legal issues. The first part of the 21st century will likely go down in history as the era when ethical hackers opened governments and the line of transparency moved by force. One need only read the motto "we open governments" on the Twitter page for Wikileaks to gain a sense of the sea change that has occurred. Ethical hacking is the non-violent use of a technology in pursuit of a cause—political or otherwise—which is often legally and morally ambiguous. Hacktivists believe in two general but spirited principles: respect for human rights and fundamental freedoms, including freedom of expression and personal privacy; and the responsibility of government to be open, transparent and fully accountable to the public. How courts and governments will deal with hacking attempts which operate in a grey zone of the law and where different ethical views collide remains to be seen. What is undisputed is that Ethical Hacking presents a fundamental discussion of key societal questions. A fundamental discussion of key societal questions. This book is published in English. - La première moitié du XXIe siècle sera sans doute reconnue comme l'époque où le piratage éthique a ouvert de force les gouvernements, déplaçant les limites de la transparence. La page twitter de Wikileaks enchâsse cet ethos à même sa devise, « we open governments », et sa volonté d'être omniprésent. En parallèle, les grandes sociétés de technologie comme Apple se font compétition pour produire des produits de plus en plus sécuritaires et à protéger les données de leurs clients, alors même que les gouvernements tentent de limiter et de décrypter ces nouvelles technologies d'encryption. Entre-temps, le marché des vulnérabilités en matière de sécurité augmente à mesure que les experts en sécurité informatique vendent des vulnérabilités de logiciels des grandes technologies, dont Apple et Google, contre des sommes allant de 10 000 à 1,5 million de dollars. L'activisme en sécurité est à la hausse. Le piratage éthique est l'utilisation non-violence d'une technologie quelconque en soutien d'une cause politique ou autre qui est souvent ambigue d'un point de vue juridique et moral. Le hacking éthique peut désigner les actes de vérification de pénétration professionnelle ou d'experts en sécurité informatique, de même que d'autres formes d'actions émergentes, comme l'hacktivisme et la désobéissance civile en ligne. L'hacktivisme est une forme de piratage éthique, mais également une forme de militantisme des droits civils à l'ère numérique. En principe, les adeptes du hacktivisme croient en deux grands principes : le respect des droits de la personne et les libertés fondamentales, y compris la liberté d'expression et à la vie privée, et la responsabilité des gouvernements d'être ouverts, transparents et pleinement redevables au public. En pratique, toutefois, les antécédents comme les agendas des hacktivistes sont fort diversifiés. Il n'est pas clair de quelle façon les tribunaux et les gouvernements traiteront des tentatives de piratage eu égard aux zones grises juridiques, aux approches éthiques conflictuelles, et compte tenu du fait qu'il n'existe actuellement, dans le monde, presque aucune exception aux provisions, en matière de cybercrime et de crime informatique, liées à la recherche sur la sécurité ou l'intérêt public. Il sera également difficile de déterminer le lien entre hacktivisme et droits civils. Ce livre est publié en anglais.
Digital Fingerprinting - Cliff Wang 2016-10-25
This is the first book on digital fingerprinting that comprehensively covers the major areas of study in a range of information security areas including authentication schemes, intrusion detection, forensic analysis and more. Available techniques for assurance

are limited and authentication schemes are potentially vulnerable to the theft of digital tokens or secrets. Intrusion detection can be thwarted by spoofing or impersonating devices, and forensic analysis is incapable of demonstrably tying a particular device to specific digital evidence. This book presents an innovative and effective approach that addresses these concerns. This book introduces the origins and scientific underpinnings of digital fingerprinting. It also proposes a unified framework for digital fingerprinting, evaluates methodologies and includes examples and case studies. The last chapter of this book covers the future directions of digital fingerprinting. This book is designed for practitioners and researchers working in the security field and military. Advanced-level students focused on computer science and engineering will find this book beneficial as secondary textbook or reference.