cryptography

MDPI

Book Review

Privacy in a Digital, Networked World: Technologies, Implications and Solutions. By Sherali Zeadally and Mohamad Badra. Springer International Publishing: 418 pp.; $51.89; ISBN-10: 3319084690, ISBN-13: 978-3319084695

Nicolas Sklavos

Computer Engineering and Informatics Department, University of Patras, 26504 Patras, Greece; nsklavos@ceid.upatras.gr

Academic Editor: Kwangjo Kim
Received: 13 March 2017; Accepted: 16 March 2017; Published: 19 March 2017

The book entitled *Privacy in a Digital, Networked World: Technologies, Implications and Solutions* of the series *Computer Communications and Networks* is the latest published book edited by Sherali Zeadally and Mohamad Badra. The two editors provide us with an integrated book on a plethora of issues in security from the technical, legal and ethical aspects. In this book, the reader will be informed of a variety of themes of security in: cloud computing, crowd sourcing platforms, databases, healthcare, vehicular ad hoc networks, big data, mobile devices, location-based and biometric systems, smart grid technology, social networks, behavioral economics and peer-to-peer networks.

The editors present an extensive and prosperous guide book that is organized in 16 major chapters with sub-sections and enlightening literature at the end of each chapter. At the beginning of the book, Zeadally and Badra introduce the reader to the growing interest in technological solutions, applications and system communications and underline the importance of security and privacy in our everyday life and communication on the web, which becomes greater in the case of cloud computing and big data. The second chapter, entitled "Database Privacy", refers to the case of protecting data in databases released in public while simultaneously the privacy of personal information. For this reason the Statistical Disclosure Control (SDC) discipline is proposed, with other current privacy models and anonymization techniques used by the computer science community. The third chapter, "Privacy and Big Data", talks about the importance of the protection of big data. Here the authors mention the revealing case of Edward Snowden regarding the US National Security Agency/Central Security Service's (NSA) big data surveillance programs which raised public awareness of the big data case studies. Moreover, big data analysis methods and techniques are described, with their advancements and restrictions. Apart from the various legal and ethical issues, the privacy protecting architectures of the future are proposed in this book. The fourth chapter, "Privacy in Crowd-Sourced Platforms", is about participating in successive surveys which require attention to privacy and protection of personal data. To encounter the risks from these crowd-sourced large-scale platforms in matters of privacy, the authors of this chapter propose the platform prototype named "Loki". They explain the basic protocol and the system components, from design to evaluation, based on a survey of the existing solutions. This is a research area that needs further investigation. The next chapter, called "Privacy in Healthcare", is dedicated to the electronic systems in the field of healthcare. Except for the competitive advantage of remote access to health care information for the users/patients, there are several challenges in protecting and securing the personal data that concern health issues and medical treatment. Several health care systems are tested on matters of privacy and, therefore, a few systems that can address the challenges highlighted are recommended here. The sixth chapter, "Privacy in

Peer-to-Peer Networks", concerns issues about privacy in this area. The authors focus on Peer to Peer (P2P) networks and applications which do not offer much privacy protection since data are stored in peers that can be openly accessed and used. For this reason, the authors present solutions and mechanisms for coping with this privacy issue. The seventh chapter has the title "Privacy in the Cloud". The authors present a survey about wide-area access to services and resources by using the cloud. These services may be very popular and are used by individuals and companies for flexibility and cost-efficiency. Beyond the advantages and adaptability of cloud computing, there are serious flaws when it comes to privacy. In this chapter, techniques for confronting these new attacks, which make the confidentiality and privacy of data vulnerable, are explored. The eighth chapter, "Privacy in Vehicular Ad Hoc Networks", refers to a new technology for traffic accidents, concerning their prevention and elimination. Vehicular Ad-hoc NETworks (VANETs) offer a great variety of applications that change our way of thinking about road safety. Besides their informative characteristics, these applications should be controlled for security and privacy as well. The idea is adapting the use of public key infrastructures (PKIs) in the VANET environment. At the end of the chapter, the challenges and opportunities in VANETs are discussed, including security issues such as anonymity, pseudonymity, unlinkability, and minimal information disclosure. The ninth chapter, entitled "Privacy Law and Regulation: Technologies, Implications, and Solutions", talks about the legislature that has been enacted to protect personal data. This chapter discusses the laws that help consumers to protect their personal information from retrieval, collection and exploitation. Here the authors present the state of privacy law (constitutional, common law and statutory foundations of privacy) in the United States and in Europe, respectively. Then they make a comparative analysis of the differences between EU regulations for privacy and those of the US and they offer suggestions for principles in privacy policies. The next chapter has the title "Privacy in Mobile Devices", concerning the privacy issues in the mobile ecosystem. Problems that arise in data protection in mobile applications are discussed and the best practices and methods to prevent data collection and control access to personal information are proposed. The 11th chapter, "Privacy in Biometric Systems", is about biometrics-reliant applications for determining misrepresentation and forgery. To address the problems of security and privacy, the authors discuss possible solutions and current trends to enhance privacy when using biometric systems. The next chapter has the title "Privacy in Social Networks" and talks about the favored social networks that have taken the world by storm in recent years. Many people upload and share a large amount of personal information on a daily basis and this is something that does not slip past the attackers' attention. Methods to secure and protect these personal data when using web 2.0 technology are proposed. The title of chapter 13 is "The Right to Privacy in the Age of Digital Technology". It is a general analysis on the importance of privacy in our digital era and how this right should be protected and defended by law in our times. The 14th chapter is entitled "How to Explore Consumers' Privacy Choices with Behavioral Economics" and demonstrates tools and ways for stakeholders, developers and practitioners to use in order to fathom the consumers' privacy behaviors and relevant experiments to develop. Chapter number 15 is "Techniques, Taxonomy, and Challenges of Privacy Protection in the Smart Grid". This chapter analyzes the operations and characteristics of the smart grid (SG) and how information can be transmitted successfully from the traditional schema of the power grid to the novel smart grid. Thus, a taxonomy is developed that can be used in confronting the privacy concerns and future challenges. The last chapter has the title "Location-Based Privacy, Protection, Safety, and Security", and the authors talk about privacy and security, and especially about privacy protection in location-based services. They carefully explain the effectiveness of applying the location-based privacy solution, while paying attention to the meaning of "privacy" and "privacy protection".

This is a comprehensive book that provides students, specialists, researchers and non-professionals with a special interest in privacy with significant groundwork in learning, together with comprehensive access to the latest developments in privacy for several emerging technologies in the 21st century. Through the extensive literature, figures and examples, the learner is able to comprehend the various

issues of privacy and security described in this book and apply a wide range of privacy protection solutions to address them in the real world.

Conflicts of Interest: The author declares no conflict of interest.