Texts in Computer Science

For other titles published in this series, go to
www.springer.com/series/3191

Joseph Migga Kizza

Ethical and Social Issues in the Information Age

Springer

Prof. Joseph Migga Kizza
Department of Computer Science and Engineering
University of Tennessee
Chattanooga, TN
USA
joseph-kizza@utc.edu

Series Editors:

David Gries
Department of Computer Science
Cornell University
Ithaca, NY
USA

Fred B. Schneider
Department of Computer Science
Cornell University
Ithaca, NY
USA

ISBN 978-1-84996-037-3 e-ISBN 978-1-84996-038-0
DOI 10.1007/978-1-84996-038-0
Springer London Dordrecht Heidelberg New York

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Control Number: 2010920467

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface to the Fourth Edition

The frequency of new editions of this book is indicative of the rapid and tremendous changes in the fields of computer and information sciences. First published in 1995, the book has rapidly gone through three editions already and now we are in the fourth. Over this period, we have become more dependent on computer and telecommunication technology than ever before and computer technology has become ubiquitous. Since I started writing on social computing, I have been advocating a time when we, as individuals and as nations, will become totally dependent on computing technology. That time is almost on us. Evidence of this is embodied in the rapid convergence of telecommunication, broadcasting, and computing devices; the miniaturization of these devices; and the ever increasing storage capacity, speed of computation, and ease of use. These qualities have been a big pulling force sucking in millions of new users every day, sometimes even those unwilling. Other appealing features of these devices are the increasing number of applications, *apps*, as they are increasingly becoming known, and being wireless and easily portable. Whether small or big, these new gizmos have become the centerpiece of an individual's social and economic activities and the main access point for all information. Individuals aside, computing technology has also become the engine that drives the nations' strategic and security infrastructures that control power grids, gas and oil storage facilities, transportation, and all forms of national communication, including emergency services. These developments have elevated cyberspace to be the most crucial economic and security domains of nations.

US President Barack Obama has classified cyberspace security and cyber threat as one of the most serious economic and national security challenges the United States is facing as a nation.[1] He, in particular, classified the country's computer networks to be the national security priority. What led to this has been a consistent and growing problem of cyber threats. In 2007 alone, the Pentagon reported nearly 44,000 incidents of malicious cyber activities carried out by foreign militaries, intelligence agencies, and individual hackers.

In April 2009, the US government admitted, after reports, that the nation's power grid is vulnerable to cyber attack, following reports that it has been infiltrated by foreign spies. According to reports, there is a pretty strong consensus in the security

[1] "US 'concerned' over cyber threat". http://news.bbc.co.uk/2/hi/americas/8126668.stm

community that the SCADA (*Supervisory Control And Data Acquisition*), an industrial control system that is used to monitor and control industrial, infrastructure, or facility-based processes, has not kept pace with the rest of the industry; it needs, if not total replacement, at least a detailed update to keep abreast of rapid changes in technology. According to the *Wall Street Journal*, the intruders had not sought to damage the power grid or any other key infrastructure so far, but suggested that they could change their approach in the event of a crisis or war. The motives behind these potential attacks are undoubtedly military, economic, and political.[2] There are almost similar stories with other countries.

The rising trend in cyber attacks, many of them with lightening speed, affecting millions of computers worldwide and in the process causing a loss of billions of dollars to individuals and businesses, may be an indication of how unprepared we are to handle such attacks not only now but also in the future. It may also be a mark of the poor state of our cyberspace security policies and the lack of will to implement these policies and develop protocols and build facilities that will diminish the effects of these menacing activities if not eliminating them altogether.

It is encouraging though to hear that at last governments have started to act. For example, the US government has started to take all aspects of cyber crime very seriously and the department of defense (DoD) has formed an entire cyber command to handle online threats to the country. The United Kingdom (UK) has also launched a cyber defense program and both countries are in possession of and are building more effective cyber warfare capabilities. They are not the only one. This is not limited to the United States and the United Kingdom alone; a number of other countries including China and Russia are also building their own capabilities. There is a growing realization that the next big war may probably be fought in cyberspace. One hopes, though, that as these governments prepare defensive stances, they also take steps to protect the individual citizens.

As we look for such defensive strategies, the technological race is picking up speed with new technologies that make our efforts and existing technologies on which these strategies based obsolete in shorter and shorter periods. All these illustrate the speed at which the computing environment is changing and demonstrate a need for continuous review of our defensive strategies and more importantly a need for a strong ethical framework in our computer, information and engineering science education. This has been the focus of this book and remains so in this edition.

What Is New in This Edition

There has been considerable changes in the contents of the book to bring it in line with the new developments we discussed above. In almost every chapter, new content has been added and we have eliminated what looked as outdated materials.

[2] Maggie Shiels. “Spies ‘infiltrate US power grid’”.
Thursday, 9 April 2009 http://news.bbc.co.uk/2/hi/technology/7990997.stm

Since content in some chapters had not changed since the first edition, this was an opportunity to bring all chapter contents up to date. In addition to new chapter contents, chapter objectives have been added to streamline chapter content to give it a telescoping view for the student to look forward to. I also wanted to make the reading of chapters more interactive by including, sporadically, **Issues for Discussion**, a series of thought-provoking questions and statements. These are intended to ignite students' interest beyond the entrance scenarios that open up the book chapters and start classroom discussions.

Chapter Overview

The book is divided into 14 chapters as follows:

Chapter 1—History of Computing (New) gives an overview of the history of computing science in hardware, software, and networking, covering pre-historic (prior to 1946) computing devices and computing pioneers since the *Abacus*. It also discusses the development of computer crimes and the current social and ethical environment. Further, computer ethics is defined, and a need to study computer ethics is emphasized.

Chapter 2—Morality and the Law defines and examines personal and public morality, identifying assumptions and value the law, looking at both conventional and natural law, and the intertwining of morality and the law. It, together with Chapter 3, gives the reader the philosophical framework needed for the remainder of the book.

Chapter 3—Ethics and Ethical Analysis (New) builds upon Chapter 2 in setting up the philosophical framework and analysis tools for the book discussing moral theories and problems in ethical relativism. Based on these and in light of the rapid advances in technology, the chapter discusses the moral and ethical premises and their corresponding values in the changing technology arena.

Chapter 4—Ethics and the Professions (changed) examines the changing nature of the professions and how they cope with the impact of technology on their fields. An ethical framework for decision making is developed. Professional and ethical responsibilities based on community values and the law are also discussed. And social issues including harassment and discrimination are thoroughly covered.

Chapter 5—Anonymity, Security, Privacy and Civil Liberties surveys the traditional ethical issues of privacy, security, anonymity and analyzes how these issues are affected by computer technology. Information gathering, databasing, and civil liberties are also discussed.

Chapter 6—Intellectual Property Rights and Computer Technology discusses the foundations of intellectual property rights and how computer technology has influenced and changed the traditional issues of property rights, in particular intellectual property rights.

Chapter 7—Social Context of Computing considers the three main social issues in computing namely, the digital divide, workplace issues like employee monitoring, and health risks, and how these issues are changing with the changing computer technology.

Chapter 8—Software Issues: Risks and Liabilities revisits property rights, responsibility, and accountability with a focus on computer software. The risks and liabilities associated with software and risk assessment are also discussed.

Chapters 9—Computer Crimes surveys the history and examples of computer crimes, their types, costs on society, and strategies of detection and prevention.

Chapter 10—New Frontiers for Ethical Consideration: Artificial Intelligence, Cyberspace, and Virtual Reality discusses the new frontiers of ethics: virtual reality, artificial intelligence, and the Internet, and how these new frontiers are affecting the traditional ethical and social issues.

Chapter 11—Cyberspace and Cyberethics and Social Networking (New) discusses the new realities of global computer networks, the intertwining of global economies, monopolies and their economic implications, globalization, emerging issues like global ethics, culture, and the development of the lingua franca for the Internet. It also focuses the discussion on the new realities of social networking.

Chapter 12—Computer Networks and Online Crimes begins by presenting the core basics of computer networks for those readers who have never taken a course in computer networks. Then the chapter discusses the major online crimes and ends by a discussion of techniques and technologies in use to mitigate these crimes.

Chapter 13—Computer Crime Investigations discusses what constitutes digital evidence, the collection and analysis of digital evidence, chain of custody, the writing of the report, and the possible appearance in court as an expert witness.

Chapter 14—Biometrics starts by discussing the different techniques in access control. Biometric technologies and techniques are then introduced to be contrasted with the other known techniques. Several biometrics and biometric technologies are discussed.

Audience

The book satisfies the new **Computer Science curriculum 2008: An Interim Revision of CS 2001**, which includes updates of the **CS2001 Computer/Science Curricula for undergraduates: Social and Professional Issues/(SP)**. This new curriculum is intended for computer science, information science, and software engineering students. Students in related disciplines like computer information and information management systems, and library sciences will also find this book informative.

It is also good for anyone interested in knowing how ethical and social issues like privacy, civil liberties, security, anonymity, and workplace issues like harassment and discrimination are affecting the new computerized environment.

In addition, anybody interested in reading about computer networking, social networking, information security, and privacy will also find the book very helpful.

Acknowledgments

I appreciate all the help I received from colleagues who offered ideas, criticism, sometimes harsh, and suggestions from anonymous reviewers over the years. Special thanks to my dear wife, Dr. Immaculate Kizza, who offered a considerable amount of help in proofreading, constructive ideas, and wonderful support.

Chattanooga, TN, USA Joseph Migga Kizza

Contents