Texts in Computer Science

Editors
David Gries
Fred B. Schneider

For further volumes:
http://www.springer.com/series/3191

Joseph Migga Kizza

Ethical and Social Issues in the Information Age

Fifth Edition

Springer

Joseph Migga Kizza
Department of Computer Science
and Engineering
University of Tennessee
Chattanooga, TN
USA

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

ISSN 1868-0941 ISSN 1868-095X (electronic)
ISBN 978-1-4471-4989-7 ISBN 978-1-4471-4990-3 (eBook)
DOI 10.1007/978-1-4471-4990-3
Springer London Heidelberg New York Dordrecht

Library of Congress Control Number: 2013934588

Printed on acid-free paper

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

Preface to the Fifth Edition

We may have experienced the fastest growth of technology in the last 10 years than ever before. Tremendous technological advances have been registered across the board from telecommunication with jaw-dropping developments in computing and telecommunication creating the long expected convergency of communications and computing platforms that are reaching into all remote corners of the world, bringing the poor and less affluent to per with the rest of the developed world. Along the way, these new technological developments have created new communities and ecosystems that are themselves evolving, in flux and difficult to secure and with questionable, if not evolving ethical systems that will take us time to learn, if it remains constant at all. Because of these rapid and unpredictable changes, my readers across the world have been contacting me to revise the contents of the book that has so far stood the currents now for 17 years. The frequency of new editions of this book is a testimony to these rapid and tremendous technological changes in the fields of computer and telecommunication sciences. First published in 1995, the book has rapidly gone through four editions already and now we are in the fifth. During that time, 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, computing and mobile devices, the miniaturization of these devices, 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 increasing number of applications, *apps*, as they are increasingly becoming known, and their being wireless and easily portable. Whether small or big, these new gismos have become a center piece 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. The U.S. government has classified cyberspace security and cyber threat as one of the most serious economic and national security challenges the U.S. is facing as a nation.[1] This, in particular, classifies the country's computer networks as national security priority. What led to this has been a consistent and growing problem of cyber threats. In his article, "New Security Flaws Detected in Mobile Devices", Byron Acohido,[2] reports of the two recent examinations by Cryptography Research, the company that did the research, of mobile devices that revealed gaping security flaws. In one study, Cryptography Research showed how it's possible to eavesdrop on any Smartphone or tablet as it is being used to make a purchase, conduct online banking or access a company's virtual private network. Also, McAfee, an anti-virus software company and a division of Intel, showed ways to remotely hack into Apple iOS and steal secret keys and passwords, and pilfer sensitive data, including call histories, e-mail and text messages. What is more worrying is the reported fact that the device under attack would not in anyway show that an attack is underway. Almost every mobile system user, security experts and law enforcement officials are all anticipating that cybergangs will accelerate attacks as consumers and companies begin to rely more heavily on mobile devices for shopping, banking and working. To make this even more complicated is the growing geographical sources of such cybergangs, now spanning the whole globe with patches of geo-political laws, in reality unenforceable. So there is an urgent need for a broader array of security awareness, at a global scale, of communities and actions by these communities to assist in providing all users the highest level of protection.

In April 2009, the U.S. 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 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 and needs, if not total replacement, 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.[3] 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 billions of dollars in

[1] "US 'concerned' over cyber threat". http://news.bbc.co.uk/2/hi/americas/0000008.stm

[2] Byron Acohido, "New Security Flaws Detected in Mobile Devices". http://www.enterprise-security-today.com/news/Mobile-Devices-Vulnerable-to-Attack/story.xhtml?story_id=0000003FAI65, April 10, 0002.

[3] Maggie Shiels. "Spies 'infiltrate US power grid'".

Thursday, 9 April 0009 http://news.bbc.co.uk/2/hi/technology/0000007.stm losses 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 the will to implement these policies and develop protocols and build facilities that will diminish the effects of these menacing activities if not eliminating them all together.

It is encouraging though to hear that at long last governments have started to act. For example, the U.S. 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 ones. This is not limited to U.S. and UK but a number of other countries including China and Russia are 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, that 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 and what seems to be repeated materials. Because of the bedrock moral values and the enduring core ethical values of our community, the content in some chapters had not changed since the first edition. Because the popularity of *Issues for Discussion*, a series of thought provoking questions and statements, meant to make the reading of chapters more interactive, this series has been kept in this edition. But of more interest to our readers is the addition of three new chapters dealing with the growing areas of technology. These are Chaps. 11 on *Virtualization*, 13 on *Ethical, Privacy and Security in the Online Social Networks Ecosystems* and 14 on *Mobile Systems and Their Intractable Social, Ethical and Security Issues*. The discussion throughout is candid intended to ignite students interest, participation in class discussions of the issues and beyond.

Chapter Overview

The book is divided into 16 chapters as follows:

Chapter 1—History of Computing gives an overview of the history of computing science in hardware, software, and networking, covering pre-historic (prior to 0006) 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 values of the law, looking at both conventional and natural law, and the intertwining of morality and the law. It, together with Chap. 3, gives the reader the philosophical framework needed for the remainder of the book.

Chapter 3—Ethics and Ethical Analysis builds upon Chap. 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 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 Computer Ethics: Artificial Intelligence discusses the new frontiers of ethics in the new intelligent technologies and how these new frontiers are affecting the traditional ethical and social issues (New).

Chapter 11—New Frontiers for Computer Ethics: Virtualization and Virtual Reality (New) discusses the new developments and consequences of the virtualization technology and its implications on our participation and how the technology informs our behavior based on our traditional moral and ethical values.

Chapter 12—New Frontiers for Computer Ethics: Cyberspace discusses the new frontiers of ethics in cyberspace and the Internet, and how these new frontiers are affecting the traditional ethical and social issues.

Chapter 13—Ethical, Privacy, and Security Issues in the Online Social Network Ecosystem (New) discusses the new realities of global computer social network ecosystems, global linguistic, cultural, moral, and ethical dynamisms, and their impact on our traditional and cherished moral and ethical systems.

Chapter 14—Mobile Systems and Their Intractable Social, Ethical and Security Issues (New) begins by presenting rather a frightening and quickly evolving mobile telecommunication and computing technologies, their unprecedented global reach and inclusion, unparalleled social, financial, and cultural prowess and the yet to be defined social, moral, and ethical value systems.

Chapter 15—Computer Crime Investigations and Ethics 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. Ethical implications of these processes, the role of the legal framework, and the absence of an ethical framework are discussed in depth.

Chapter 16— Biometrics Technologies and Ethics 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 and their ethical implications are discussed.

Audience

The book satisfies the new *ACM/IEEE-CS Computer Science Curricula 2013, (CS2013)'s Social and Professional Practice (SP)*, a draft of which is found at: http://ai.stanford.edu/users/sahami/CS2013/strawman-draft/cs2013-strawman.pdf. The CS2013 focuses on the need for any Computer Science undergraduate to understand the basic cultural, social, legal, and ethical issues inherent in the discipline of computing. To do this, they need to:

- Understand where the discipline has been, where it is, and where it is heading
- Understand their individual roles in this process, as well as appreciate the philosophical questions, technical problems, and aesthetic values that play an important part in the development of the discipline
- Develop the ability to ask serious questions about the social impact of computing and to evaluate proposed answers to those questions
- Be aware of the basic legal rights of software and hardware vendors and users, and they also need to appreciate the ethical values that are the basis for those rights

Students in related disciplines like computer information and information management systems and library sciences will also find this book informative.

The book is also good for Computer Science practitioners who must practice the principles embedded in the CS2013 curriculum based on understanding:

- The responsibility that they bear and the possible consequences of failure.
- Their own limitations as well as the limitations of their tools.

The book 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.

Department of Computer Science and Engineering
University of Tennessee, Chattanooga
Tennessee, USA

Joseph Migga Kizza

Contents