
Undergraduate Topics in Computer Science

Series editor

Ian Mackie

Advisory Board

Samson Abramsky, University of Oxford, Oxford, UK

Chris Hankin, Imperial College London, London, UK

Mike Hinchey, University of Limerick, Limerick, Ireland

Dexter C. Kozen, Cornell University, Ithaca, USA

Andrew Pitts, University of Cambridge, Cambridge, UK

Hanne Riis Nielson, Technical University of Denmark, Kongens Lyngby, Denmark

Steven S. Skiena, Stony Brook University, Stony Brook, USA

Iain Stewart, University of Durham, Durham, UK

Undergraduate Topics in Computer Science (UTiCS) delivers high-quality instructional content for undergraduates studying in all areas of computing and information science. From core foundational and theoretical material to final-year topics and applications, UTiCS books take a fresh, concise, and modern approach and are ideal for self-study or for a one- or two-semester course. The texts are all authored by established experts in their fields, reviewed by an international advisory board, and contain numerous examples and problems. Many include fully worked solutions.

More information about this series at <http://www.springer.com/series/7592>

Joseph Migga Kizza

Ethical and Secure Computing

A Concise Module

Second Edition

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

ISSN 1863-7310 ISSN 2197-1781 (electronic)
Undergraduate Topics in Computer Science
ISBN 978-3-030-03936-3 ISBN 978-3-030-03937-0 (eBook)
<https://doi.org/10.1007/978-3-030-03937-0>

Library of Congress Control Number: 2018961714

1st edition: © Springer International Publishing Switzerland 2016

2nd edition: © Springer Nature Switzerland AG 2019

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Following new technological developments is like climbing a mountain shrouded in early morning mist always expecting to crest at every forward step but never cresting. Yet we don't give up. We have gotten involved, to almost a point of enslavement, yet we keep on moving always expecting more and better as dire warnings of overuse fly just pass us. The overwhelming growth of technology and its ability to give us unlimited powers making us able to do things unthinkable just a few years past is equally creating as much excitement as it creates security scares and bewilderment. Tremendous technological advances have been registered across the board from telecommunication to computing with jaw-dropping developments. Along the way, these developments are creating an unprecedented convergence of communications and computing platform technologies that are reaching into all remote corners of the world, bringing the poor and less affluent on a par with the rest of the developed world. 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 time to learn, if it remains constant at all. Because of these rapid and unpredictable changes, I found my previous edition, *Ethics in Computing: A Concise Module*, in need of a review and an update. Without losing my focus and flavor of the previous edition, I have selectively updated the content of the chapters, adding new ones and clarifying the message that a time is coming, if not already here, when we, as individuals and as nations, will become totally dependent on computing technology. Evidence of this is embodied in the rapid convergence of telecommunication, broadcasting, computing and mobile devices, the miniaturization of these devices, the ever-growing ubiquity of computing, the speed of computation, and ease of use. These technology characteristics have been a big pulling force sucking in millions of new users every day, sometimes even those who are unwilling. Other appealing features of technology are ever-growing pervasiveness and applications both good and bad. Whether small or big, devices based on the growing ability of the changing technology have become the centerpiece of an individual's social and economic activities, the main access point for all information and the empowerment of the device owners. 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 the cyberspace ecosystem as the most crucial economic and security environment of nations requiring an *ethical and secure computing environment*.

As we look for ethical and secure computing strategies, the technological race is picking up speed with new technologies that make our efforts and existing protocols 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 and secure framework* in our computer, information, and engineering science education. This has been and will continue to be the focus of all my writings on this topic, and it is and remains so in this second edition.

Chapter Overview

This second edition is divided into twelve chapters as follows:

Chapter 1—**Morality and the Law** defines and examines the personal and public morality, identifying assumptions and values of the law, looking at both conventional and natural laws, 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 2—**Ethics and Ethical Analysis** sets 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 3—**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 to help in 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 4—**Anonymity, Security, and 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 5—**Intellectual Property Rights and Computer Technology** discusses the foundations of intellectual property rights and how computer technology has influenced and continues to influence and change the traditional issues of property rights, in particular intellectual property rights.

Chapter 6—**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 7—**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.

Chapter 8—**Computer Crimes** surveys the history and examples of computer crimes, their types, costs on society, and strategies of detection and prevention.

Chapter 9—**Cyberbullying** discusses the growing threat and the effects of repeated deliberate harm or harassment of other people by using electronic technology that may include devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and Web sites.

Chapter 10—**Evolving Realities: Ethical and Secure Computing in the New Technological Spaces** discusses the new frontiers of ethical and secure computing in the new technological spaces that include intelligent and virtualization technologies, virtual spaces and realities, and their effects on the traditional ethical and social fabric of society.

Chapter 11—**Ethical, Privacy, and Security Issues in Online Social Network Ecosystem** discusses the new realities of global computer social network ecosystems, global linguistic, cultural, moral, and ethical dynamics, and their impact on our traditional and cherished moral and ethical systems.

Chapter 12—**Evolving Cyberspace: The Marriage of 5G and the Internet of Things (IoT) Technologies (New)** discusses the new frontiers of ethical and secure computing in the new and developing Internet–user interface whose protocols, policies, and standards are yet to be defined, discussed, and accepted by the scientific and user communities. We will explore how this new interface has created an ethical and security quagmire and how this is affecting our traditional ethical and social systems.

Audience

The book satisfies the following ACM/IEEE Curricula (i) CS-Computer Science Curriculum 2015 and (ii) CS-Information Technology Curriculum 2017 (<https://www.acm.org/binaries/content/assets/education/curricula-recommendations/it2017.pdf>). In summary, all these curricula emphasize the student’s understanding of the basic cultural, social, legal, and ethical issues inherent in the discipline of computing. To achieve this, the student must:

- understand where the discipline has been, where it is, and where it is heading.
- understand the 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 the 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 curricula 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, mobile computing, social networking, information security, and privacy will also find the book very helpful.

Acknowledgements

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
2018

Joseph Migga Kizza

Contents

1	Morality and the Law	1
1.1	Introduction	2
1.2	Morality	3
1.2.1	Moral Theories	4
1.2.2	Moral Decision Making	4
1.2.3	Moral Codes	5
1.2.4	Moral Standards	8
1.2.5	Guilt and Conscience	8
1.2.6	Morality and Religion	9
1.3	Law	9
1.3.1	The Natural Law	10
1.3.2	Conventional Law	11
1.3.3	The Purpose of Law	11
1.3.4	The Penal Code	12
1.4	Morality and the Law	12
1.5	Morality, Etiquettes, and Manners	14
	References	16
2	Ethics and Ethical Analysis	17
2.1	Traditional Definition	18
2.2	Ethical Theories	19
2.2.1	Consequentialism	19
2.2.2	Deontology	20
2.2.3	Human Nature	20
2.2.4	Relativism	21
2.2.5	Hedonism	21
2.2.6	Emotivism	21
2.3	Functional Definition of Ethics	22
2.4	Ethical Reasoning and Decision Making	24
2.4.1	A Framework for Ethical Decision Making	25
2.4.2	Making and Evaluating Ethical Arguments	25

2.5	Codes of Ethics	27
2.5.1	2018 ACM Code of Ethics and Professional Conduct: Draft 1	27
2.5.2	Objectives of Codes of Ethics	28
2.6	Reflections on Computer Ethics	28
2.6.1	New Wine in an Old Bottle	28
2.7	Technology and Values	31
	References	33
3	Ethics and the Professions	35
3.1	Introduction	36
3.2	Evolution of Professions	37
3.2.1	Origins of Professions	37
3.2.2	Requirements of a Professional	37
3.2.3	Pillars of Professionalism	39
3.3	The Making of an Ethical Professional: Education and Licensing	43
3.3.1	Formal Education	43
3.3.2	Licensing Authorities	45
3.3.3	Professional Codes of Conduct	45
3.4	Professional Decision Making and Ethics	48
3.4.1	Professional Dilemmas in Decision Making	48
3.4.2	Guilt and Making Ethical Decisions	50
3.5	Professionalism and Ethical Responsibilities	52
3.5.1	Whistle-Blowing	52
3.5.2	Harassment and Discrimination	55
3.5.3	Ethical and Moral Implications	55
	References	57
4	Anonymity, Security, Privacy, and Civil Liberties	59
4.1	Introduction	62
4.2	Anonymity	63
4.2.1	Anonymity and the Internet	63
4.2.2	Advantages and Disadvantages of Anonymity	64
4.2.3	Legal View of Anonymity	64
4.3	Security	65
4.3.1	Physical Security	65
4.3.2	Physical Access Controls	66
4.3.3	Information Security Controls	67
4.3.4	Operational Security	71
4.4	Privacy	71
4.4.1	Definition	71
4.4.2	Types of Privacy	71
4.4.3	Value of Privacy	73

4.4.4	Privacy Implications of the Database System	74
4.4.5	Privacy Violations and Legal Implications	75
4.4.6	Privacy Protection and Civil Liberties	78
4.5	Ethical and Legal Framework for Information	80
4.5.1	Ethics and Privacy	80
4.5.2	Ethical and Legal Basis for Privacy Protection	81
	References	82
5	Intellectual Property Rights and Computer Technology	85
5.1	Definitions	86
5.2	Computer Products and Services	86
5.3	Foundations of Intellectual Property	89
5.3.1	Copyrights	89
5.3.2	Patents	92
5.3.3	Trade Secrets	93
5.3.4	Trademarks	95
5.3.5	Personal Identity	97
5.4	Ownership	98
5.4.1	The Politics of Ownership	99
5.4.2	The Psychology of Ownership	99
5.5	Intellectual Property Crimes	100
5.5.1	Infringement	100
5.5.2	The First-Sale Doctrine	102
5.5.3	The Fair Use Doctrine	102
5.6	Protection of Ownership Rights	102
5.6.1	Domain of Protection	103
5.6.2	Source and Types of Protection	103
5.6.3	Duration of Protection	104
5.6.4	Strategies of Protection	104
5.7	Protecting Computer Software Under the IP	105
5.7.1	Software Piracy	105
5.7.2	Protection of Software Under Copyright Laws	106
5.7.3	Protection of Software Under Patent Laws	107
5.7.4	Protection of Software Under Trademarks	107
5.7.5	Protection of Software Under Trade Secrets	108
5.8	Transnational Issues and Intellectual Property	108
	References	110
6	Social Context of Computing	113
6.1	Introduction	114
6.2	The Digital Divide	115
6.2.1	Access	116
6.2.2	Technology	123
6.2.3	Humanware (Human Capacity)	126

6.2.4	Infrastructure	127
6.2.5	Enabling Environments	127
6.3	Obstacles to Overcoming the Digital Divide	128
6.4	ICT in the Workplace	129
6.4.1	The Electronic Office	129
6.4.2	Office on Wheels and Wings	130
6.4.3	The Virtual Workplace	130
6.4.4	The Quiet Revolution: The Growth of Telecommuting	131
6.4.5	Employee Social and Ethical Issues	135
6.5	Employee Monitoring	136
6.5.1	Workplace Privacy and Surveillance	137
6.5.2	Electronic Monitoring	139
6.6	Employee Health and Productivity in the Workplace	142
6.6.1	Ergonomics	143
	References	146
7	Software Issues: Risks and Liabilities	149
7.1	Definitions	150
7.1.1	Standards	150
7.1.2	Reliability	151
7.1.3	Security	152
7.1.4	Safety	153
7.1.5	Quality	154
7.1.6	Quality of Service	154
7.2	Causes of Software Failures	154
7.2.1	Human Factors	155
7.2.2	Nature of Software: Complexity	155
7.3	Risk	156
7.3.1	Risk Assessment and Management	157
7.3.2	Risks and Hazards in Workplace Systems	158
7.3.3	Historic Examples of Software Risks	159
7.4	Consumer Protection	165
7.4.1	Buyers' Rights	165
7.4.2	Classification of Computer Software	167
7.4.3	The Contract Option	169
7.4.4	The Tort Option	171
7.5	Improving Software Quality	173
7.5.1	Techniques for Improving Software Quality	173
7.6	Producer Protection	174
	References	175
8	Computer Crimes	177
8.1	Introduction	178

8.2	History of Computer Crimes	179
8.3	Types of Computer Systems Attacks	181
8.3.1	Penetration	181
8.3.2	Denial of Service	183
8.4	Motives of Computer Crimes	183
8.5	Costs and Social Consequences	185
8.5.1	Lack of Cost Estimate Model For Cyberspace Attacks	188
8.5.2	Social and Ethical Consequences	189
8.6	Computer Crime Prevention Strategies	190
8.6.1	Protecting Your Computer	190
8.6.2	The Computer Criminal	192
8.6.3	The Innocent Victim	192
	References	194
9	Cyberbullying	197
9.1	Definition	197
9.1.1	Legal Definition	198
9.1.2	Cyberstalking	199
9.1.3	Cyberharassment	199
9.2	Types of Cyberbullying	199
9.2.1	Harassment	199
9.2.2	Flaming	200
9.2.3	Exclusion	200
9.2.4	Outing	200
9.2.5	Masquerading	200
9.3	Areas of Society Most Affected by Cyberbullying	200
9.3.1	Schools	201
9.3.2	Cyberbullying in the Workplace	201
9.4	Legislation Against Cyberbullying	202
9.4.1	Federal Laws	202
9.4.2	State Laws	202
9.4.3	International Laws	203
9.5	Effects of Cyberbullying	203
9.6	Dealing with Cyberbullying	204
9.6.1	Awareness	204
9.6.2	Legislation	205
9.6.3	Community Support	205
9.7	Resources	205
	References	207
10	Evolving Realities: Ethical and Secure Computing in the New Technological Spaces	209
10.1	Introduction	211

10.2	Artificial Intelligence	212
10.2.1	Advances in Artificial Intelligence	212
10.2.2	Artificial Intelligence and Ethics	213
10.3	Virtualization	215
10.3.1	Simulated Computing Environments	216
10.3.2	Virtual Reality	216
10.3.3	Different Types of Virtual Reality	217
10.3.4	Virtualization and Ethics	218
10.4	Cyberspace and the Concept of Telepresence	221
10.4.1	Securing Cyberspace	222
10.4.2	Social Issues in Cyberspace	222
10.4.3	Privacy in Cyberspace	224
	References	227
11	Ethical, Privacy, and Security Issues in the Online Social Network Ecosystems	229
11.1	Introduction	229
11.2	Introduction to Computer Networks	230
11.2.1	Computer Network Models	230
11.2.2	Computer Network Types	232
11.3	Social Networks (SNs)	233
11.4	Online Social Networks (OSNs)	234
11.4.1	Types of Online Social Networks	235
11.4.2	Online Social Networking Services	237
11.4.3	The Growth of Online Social Networks	238
11.5	Ethical and Privacy Issues in Online Social Networks	239
11.5.1	Privacy Issues in OSNs	240
11.5.2	Strengthening Privacy in OSNs	243
11.5.3	Ethical Issues in Online Social Networks	243
11.6	Security and Crimes in Online Social Networks	247
11.6.1	Beware of Ways to Perpetrate Crimes in Online Social Networks	248
11.6.2	Defense Against Crimes in Online Social Networks	250
11.7	Proven Security Protocols and Best Practices in Online Social Networks	253
11.7.1	Authentication	254
11.7.2	Access Control	254
11.7.3	Legislation	255
11.7.4	Self-regulation	255
11.7.5	Detection	255
11.7.6	Recovery	255
	References	256

12	Evolving Cyberspace: The Marriage of 5G and the Internet of Things (IoT) Technologies	259
12.1	Introduction	260
12.2	Fifth-Generation (5G) Technology (G5)	260
12.2.1	Overview of 5G Wireless Communications	260
12.2.2	5G Network Architecture and Protocol Stack Perspectives	261
12.2.3	Technical Challenges of 5G Technology	262
12.3	The Internet of Things (IoT)	264
12.3.1	Overview and Growth of Internet of Things	265
12.3.2	Architecture and Networking of IoT	267
12.3.3	Challenges of Using TCP/IP Architecture Over the IoT	270
12.3.4	IoT Governance, Privacy, and Security Challenges	272
12.3.5	Governance and Privacy Concerns	273
12.3.6	Security Challenges	273
12.3.7	Autonomy	274
12.3.8	Computational Constraints	275
12.3.9	Discovery	275
12.3.10	Trust Relationships	276
12.4	Ethical, Social, and Legal Impacts of 5G and IoT	276
12.4.1	Environment	277
12.4.2	E-Waste	277
12.4.3	Conflict Minerals	277
12.4.4	Healthy Issues Emanating from 5G and IoT Technologies	277
12.4.5	Ethics	277
12.5	Exercises	278
12.6	Advanced Exercises	278
	References	279
	Index	281