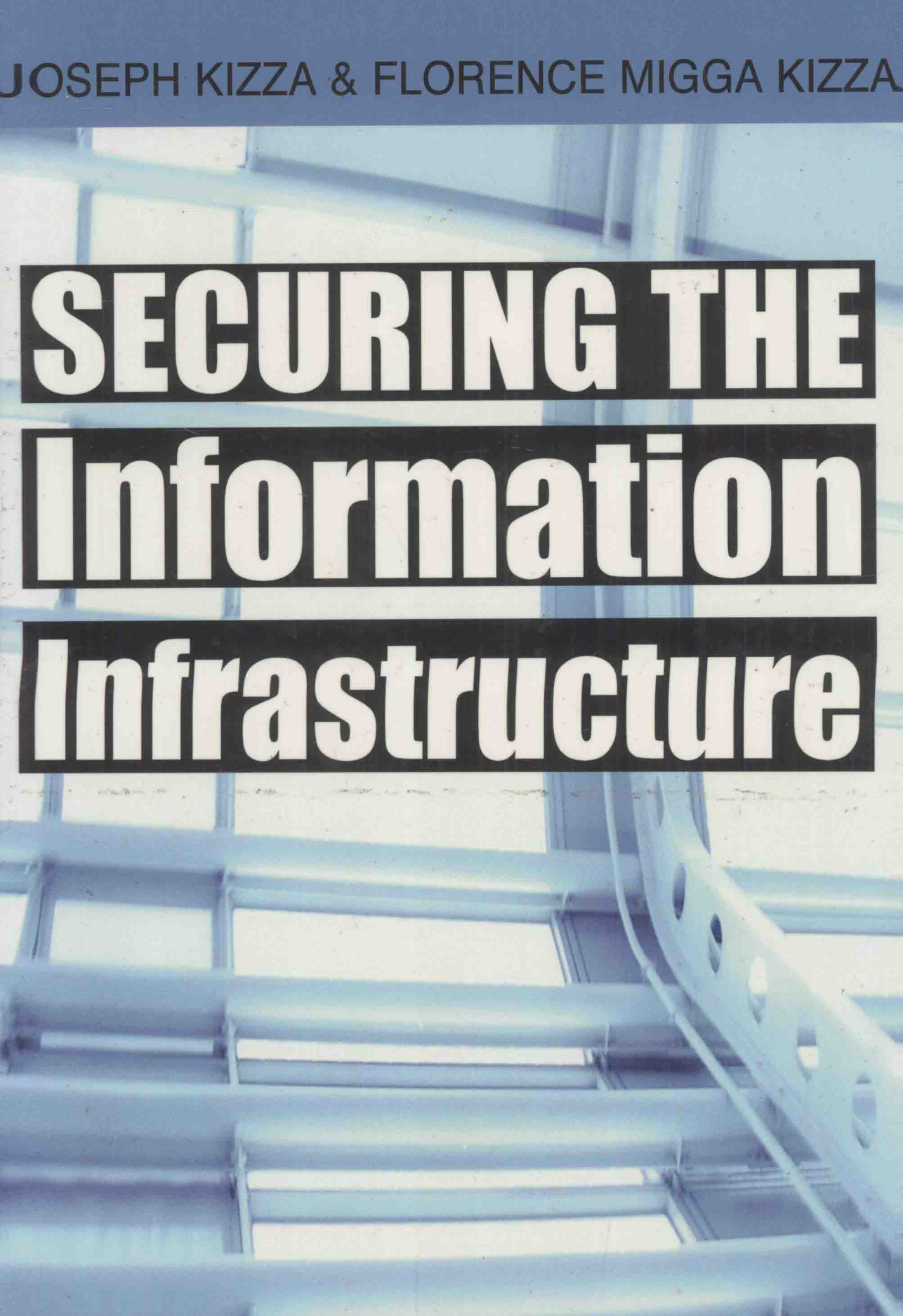


JOSEPH KIZZA & FLORENCE MIGGA KIZZA

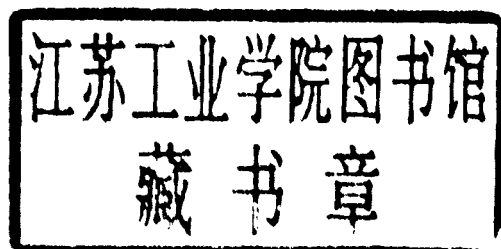


**SECURING THE  
Information  
Infrastructure**

# Securing the Information Infrastructure

Joseph M. Kizza  
University of Tennessee at Chattanooga, USA

Florence M. Kizza  
Freelance Writer, USA



**Cybertech Publishing**

Hershey • New York

Acquisition Editor: Kristin Klinger  
Senior Managing Editor: Jennifer Neidig  
Managing Editor: Sara Reed  
Development Editor: Kristin Roth  
Copy Editor: Heidi Hormel  
Typesetter: Michael Brehm  
Cover Design: Lisa Tosheff  
Printed at: Yurchak Printing Inc.

Published in the United States of America by  
CyberTech Publishing (an imprint of IGI Global)  
701 E. Chocolate Avenue  
Hershey PA 17033  
Tel: 717-533-8845  
Fax: 717-533-8661  
E-mail: [cust@igi-pub.com](mailto:cust@igi-pub.com)  
Web site: <http://www.cybertech-pub.com>

and in the United Kingdom by  
CyberTech Publishing (an imprint of IGI Global)  
3 Henrietta Street  
Covent Garden  
London WC2E 8LU  
Tel: 44 20 7240 0856  
Fax: 44 20 7379 0609  
Web site: <http://www.eurospanonline.com>

Copyright © 2008 by IGI Global. All rights reserved. No part of this book may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher.

Product or company names used in this book are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.

#### Library of Congress Cataloging-in-Publication Data

Kizza, Joseph Migga.

Securing the information infrastructure / Joseph Kizza and Florence Migga Kizza, authors.  
p. cm.

Summary: "This book examines how internet technology has become an integral part of our daily lives and as it does, the security of these systems is essential. With the ease of accessibility, the dependence to a computer has sky-rocketed, which makes security crucial"--Provided by publisher.

Includes bibliographical references and index.

ISBN 978-1-59904-379-1 (hardcover) -- ISBN 978-1-59904-381-4 (ebook)

1. Cyberterrorism. 2. Internet--Security measures. 3. Computer networks--Security measures. 4. Information superhighway--Security measures. I. Kizza, Florence Migga. II. Title.

HV6773.K59 2008  
005.8--dc22

2007007405

#### British Cataloguing in Publication Data

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

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

To Immaculate, a wonderful mother and wife

# Preface

The frequent headlines involving incidents of stolen or hacked user records from company and government institutions, like the recent Veteran Affairs episode, have brought probably unwanted attention to the constant problem of securing vital, essential, and confidential personal, business, and national records from the hands of hackers and thieves. However, to many in the security community, such news has refocused the attention of the nation, if not the whole world, and re-ignited the debate about how far we need to go and what we need to do in order to secure the information infrastructure upon which all vital information happens to reside and is transported.

Two fundamental developments have brought us to where we are today. First Internet technology has become an integral part of our daily lives, and as it has, comprehensive security for systems upon which we have come to depend has become essential. The tremendous increase in connectivity, now driven more by new Wi-Fi technologies than fixed networks, has led to an increase in remote access and consequently increased system vulnerability. These forces have, together with the plummeting prices of information processing and indexing devices and the development of sprawling global networks, made the generation, collection, processing, indexing, and storage of and access to information easy. Second, as the popularity of computer use has grown, our dependence on computers and computer technology has sky rocketed to new heights and is hovering toward total dependence. There

are serious consequences to total dependence on the information infrastructure and its associated technologies. As we have all witnessed in the last several years, Internet technologies have been like a large cruise ship in the middle of the ocean with all its enmities but without a captain. The 21<sup>st</sup> century has, thus far, the most machine-dependent generation. This dependence, though for convenience, is turning out to be one of the main sources of our security problems and a potential privacy concern. It is leading to the loss of our privacy, security, and autonomy.

These two developments, taken together, have created an even more tempting environment for online digital crimes than ever before. The annual Computer Crime Survey by the Computer Security Institute/Federal Bureau of Investigations (CSI/FBI) typically is a barometer of computer crime within the United States and every year presents alarming statistics about rising digital crime rates over our public networks. The survey results always paint a picture of cyber crimes bleeding the nation. The CSI/FBI Computer Crime and Security surveys are always targeted to computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions, and universities. Recent data from these surveys show some disturbing developments, including:

- There has been a shift from both virus attacks and denial of service, which previously outpaced all others, to theft of proprietary information.
- The percentage of organizations reporting computer intrusions to law enforcement in recent years has declined. The key reason cited for not reporting intrusions to law enforcement is the concern for negative publicity.
- Although the vast majority of the organizations view security awareness training as important, respondents from all sectors do not believe that their organizations invest enough in this area.
- Security budgets in organizations are still very low, indicating a low priority given to security.

Data like these point to perhaps the core reason why there is mounting uneasiness and fear of the developing information infrastructure. The main question arising out of this new fear is whether we should trust our new information infrastructure medium. We are at a crossroads, unable to proceed without deciding whether we should trust the path we are taking or not. If we are to trust it, how much trust must we give? Ironically, if we decide to trust, we are trusting a system we know very little about and we understand less.

Through the pages of this book, we try to give the reader reasons for trusting the information infrastructure in spite of limited user knowledge and familiarity, poor infrastructure protocol, lack of fundamental system blue prints, and its open-architecture, open-source nature. Yes, we believe that users with a strong ethical framework from a good ethics education can make sound decisions that are good for the security of the information infrastructure. Along with a strong ethical framework for decision making, we also need a tool kit of sound hardware and software security protocols and best practices that will enhance the information infrastructure's security. Finally, we believe that a strong and adoptive legal system, supported by good forensics technologies and an effective apprehension of the offenders, can create secure the environment in which we can trust the information infrastructure.

The book is, therefore, a survey of these issues in four parts. In the four chapters of Section I: Security through Moral and Ethical Education, we focus on moral and ethics education and also discuss related issues of security, privacy, and anonymity as they affect the creation of a strong ethical framework for decision making:

- In **Chapter I: Building Trust in the Information Infrastructure**, we outline the problems we as members of cyberspace are facing, problems that are challenging our individual self and society, in general. We also outline a summary of what we think is the best approach to bringing trust to an infrastructure with a runaway security problem.
- In **Chapter II: Need for Morality and Ethics**, we discussed the rising rate of computer-related crime and, in particular, information-related crimes. We point out that information infrastructure is made up of two components; the man-made component, consisting of hardware and software, and the humanware component, consisting of users. A good solution to the information infrastructure problem must address problems in both of these components.
- In **Chapter III: Building an Ethical Framework for Decision Making**, we build on the discussion in Chapter II about building a good ethical framework and its central role in securing the information infrastructure. We show that a good ethical framework is essential for good decision making.
- In **Chapter IV: Security, Anonymity, and Privacy**, we discuss the centrality of security and privacy in the information infrastructure and also the role anonymity plays. The threat to privacy and security is at the core of the problem of securing the information infrastructure. We cannot talk about a secure information infrastructure, if we cannot guarantee the security and privacy of individuals and the information on the infrastructure.

Within the 10 chapters of Section II: Security through Innovative Hardware and Software Systems, we cover all practical techniques, protocols, and best practices in use today for a secure information infrastructure. These include techniques like the issues related to software reliability and risk; security threats and vulnerabilities; information security policies and risk analysis and management; access control and authentication; firewalls, intrusion detection, and prevention; and biometrics:

- In **Chapter V: Software Standards, Reliability, Safety, and Risk**; we focus on software's role in the security of systems and how we can keep software safe, dependable, and secure, as we struggle to make the information communication infrastructure secure. Software, more than anything else, is at the heart of the information communication infrastructure. It is, in fact, one of the three main components of the infrastructure, together with hardware and humanware.
- In **Chapter VI: Network Basics and Securing the Network Infrastructure**, we give a very elementary treatment of the theory of networks and then outline the best network security solutions. This is intended to address one of the security concerns we discuss in Chapter I—users have little knowledge of the workings of the communication infrastructure.

- In **Chapter VII: Security Threats and Vulnerabilities**, we define and discuss threats and vulnerabilities for the ICT infrastructure. We do this by first identifying threats and vulnerabilities that are exploited by people like hackers.
- In **Chapter VIII: Security Policies and Risk Analysis**, we study the central role of a security policy in securing an enterprise network as has been pointed out by many security specialists, scholars, and security organizations. We further discuss several other issues about the security policy. This includes issues like what constitutes a good policy and how to formulate, develop, write, implement, and maintain a security policy.
- In **Chapter IX: Security Analysis, Assessment, and Assurance**, we look at the issues of the implantation of a security policy we discussed in Chapter VIII, starting with security assessment and analysis. The risks and potential for security breaches involving sabotage, vandalism, and resource theft are high. For security assurance of networked systems, there must be a comprehensive security evaluation to determine the status of security and ways to improve it through mitigation of security threats. So an examination and evaluation of the various factors affecting security status must be carried out and assessed to determine the adequacy of existing security measures and safeguards, and also to determine if improvements in the existing measures are needed.
- In **Chapter X: Access Control, Authentication, and Authorization**; we focus on three major security mechanisms from our security tool kit. We cover access control, authentication, and authorization.
- In **Chapter XI: Perimeter Defense: The Firewall**, we continue with our discussion of technical controls and techniques, which we started in Chapter X, by focusing on securing the perimeter of the enterprise network. This discussion consists of two parts: access control and firewalls.
- In **Chapter XII: Intrusion Detection and Prevention Systems**, we look at intrusion detection, one of the principles that defines security. Since computer networks have come to be pots of honey, attracting many, the stampede for information from computer networks is great and must be met with strong mechanisms. First there is detecting those trying to penetrate the system; second is preventing them from trying; and third is responding to the attempt, successfully or not. Although these three are the fundamental ingredients of security, most resources have been devoted to detection and prevention, because if we are able to detect all security threats and prevent them, then there is no need for a response.
- In **Chapter XIII: Security in Wireless Systems**, we follow the prediction by so many that the next dominant generation of computing technology is going to be wireless. We are already witnessing the beginning of this with the tremendous growth of wireless technology in the last few years. Along with the marvels of a new technology and more so with wireless technology, there comes an avalanche of security concerns and problems. This is also the case with wired technology. So we carefully look at the current security protocols and best practices.
- In **Chapter XIV: Biometrics for Access Control**, we look at other emerging security technologies. New technologies and new techniques must be found to create a more reliable and more secure environment. In the quest for a superior solution, biometrics verification techniques are fast emerging as the most reliable and practical method of individual identity verification. Biometrics refer to technologies and techniques that rely on measurable physiological and personal characteristics and attributes that can uniquely identify and authenticate an individual.



In the two chapters of Section III: Security through the Legal System, we discuss digital evidence and computer crime, digital crime investigations and forensics, and writing investigative reports.

- In **Chapter XV: Digital Evidence and Computer Crime**, we shift the discussion from moral and ethical education that forms an ethical framework in decision making and from implementation of security technologies, tools, and best practices, to focus on the legal and law enforcement approaches. We believe, despite the fact that the technology has outpaced the legal system and the technology the criminals use is sometimes years ahead of that of law enforcement, that the legal system can play a very positive and effective role in the security of networks and the communication infrastructure.
- In **Chapter XVI: Digital Crime Investigations and Forensics**, we focus on the investigative process. We divide the discussion into two parts. First we look at a process known as computer forensics in which we investigate crime scenes that involve data on computers. We look at the different parts of the computer and how digital evidence can be either hidden or extracted from the computer. In the second process, we consider the crime scene as not one computer but a network of computers. Our investigation then goes beyond one computer to include the infrastructure of the network and all points in the network where evidence can be either hidden or extracted. We refer to this second process as network forensics.

Finally in Section IV: What Next?, we conclude with an interesting discourse:

- In **Chapter XVII: Trends in Information Assurance**, we discuss all of the security best practices, the possible trends in security protocols and best practices, their viability, and their growth in light of rapidly developing technology. We conclude the chapter and the book by a discussion of the possibilities of new technologies and what they should cover.

We believe this kind of approach to the information infrastructure will result in a secure information infrastructure that can be trusted by all of its users and, hence, will be secured for all of us and our children to come.

*Joseph Migga Kizza*  
*Chattanooga, TN*

*Florence Migga Kizza*  
*Boca Raton, FL*

# Acknowledgment

This is a very comprehensive book covering a wide spectrum of interests in information security. It is, therefore, a challenge to the authors to present materials that will interest and challenge the majority of the intended readers. We made every effort in collecting and presenting materials that we think will go a long way to accomplish this. Along the way as we did this, we encountered many helpful and sometimes unforgettable people who went out of their way just to help by either answering one question or 10, providing a reference, questioning a statement, correcting grammar, or just pointing out a direction. We are grateful to hundreds of these unnamed heroes of this book.

Since early in its inception, this book has taken many turns and forms to get to its present form. This evolution has been a result of both content and syntax reviews, sometimes casual but many times serious. In particular, we want to thank the nameless IGI Global reviewers who made many invaluable suggestions. To all reviewers, we thank you from the bottom of our hearts for the small and large part you played. Whatever your part, you have contributed tremendously to the final product.

Finally, in a great way, we want to thank Immaculate Kizza, a mother, wife, and a gifted reviewer, for the many contributions she has made to the book. As usual you made it happen for us.



Formerly Idea Group Inc.

# Stay on the Cutting Edge of Research... with Quality, Peer-Reviewed Journals from Information Science Publishing

## International Journal of Web Services Research

Liang-jie Zhang, IBM, USA  
ISSN: 1545-7362  
EISSN: 1546-5004  
Institution: US \$475.00  
Online Only (Institution): US \$425.00  
Individual: US \$120.00

## International Journal on Semantic Web and Information Systems

Amit P. Sheth, Kno.e.sis Center, Wright State University, USA  
Miltiadis D. Lytras, Academic Research Computer Technology  
Institute, Greece  
ISSN: 1552-6283  
EISSN: 1552-6291  
Institution: US \$475.00  
Online Only (Institution): US \$425.00  
Individual: US \$115.00

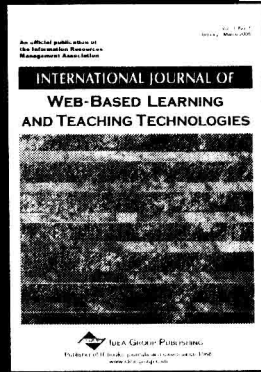
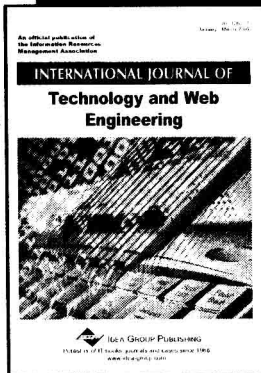
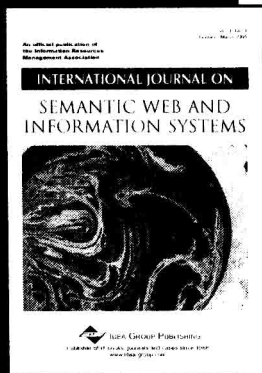
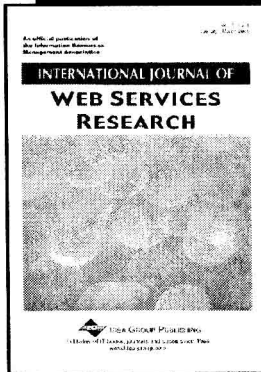
## International Journal of Information Technology and Web Engineering

Ghazi I. Alkhatib, Applied Science Univ., Amman, Jordan  
David C. Rine, George Mason University, USA  
ISSN: 1554-1045  
EISSN: 1554-1053  
Institution: US \$475.00  
Online Only (Institution): US \$425.00  
Individual: US \$110.00

## International Journal of Web-Based Learning and Teaching Technologies

Liliane Esnault, E.M.LYON, France  
ISSN: 1548-1093  
EISSN: 1548-1107  
Institution: US \$395.00  
Online Only (Institution): US \$345.00  
Individual: US \$110.00

*Institutional Print  
Subscription Includes  
FREE Online Access!*



**Download Sample Issues at**  
**[www.igi-global.com/journals](http://www.igi-global.com/journals)**

View more titles from IGI Global at [www.igi-global.com/journals](http://www.igi-global.com/journals).

Looking for a way to make information science and technology research easy? Electronic Resources are designed to keep your institution up-to-date on the latest information science technology trends and research.

# Information Technology Research at the Click of a Mouse!

## InfoSci-Online

- ⇒ Instant access to thousands of information technology book chapters, journal articles, teaching cases, and conference proceedings
- ⇒ Multiple search functions
- ⇒ Full-text entries and complete citation information
- ⇒ Upgrade to **InfoSci-Online Premium** and add thousands of authoritative entries from Information Science Reference's handbooks of research and encyclopedias!

## IGI Full-Text Online Journal Collection

- ⇒ Instant access to thousands of scholarly journal articles
- ⇒ Full-text entries and complete citation information

## IGI Teaching Case Collection

- ⇒ Instant access to hundreds of comprehensive teaching cases
- ⇒ Password-protected access to case instructor files

## IGI E-Access

- ⇒ Online, full-text access to IGI individual journals, encyclopedias, or handbooks of research

## Additional E-Resources

- ⇒ E-Books
- ⇒ Individual Electronic Journal Articles
- ⇒ Individual Electronic Teaching Cases

*Resources  
have flexible  
pricing to  
help meet the  
needs of any  
institution.*

[www.igi-online.com](http://www.igi-online.com)

*Sign Up for a  
Free Trial of  
IGI Databases!*

# Securing the Information Infrastructure

## Table of Contents

Preface.....	ix
Acknowledgment.....	xiv

### Section I: Security Through Moral and Ethical Education

<b>Chapter I</b>	
<b>Building Trust in the Information Infrastructure.....</b>	<b>1</b>
<i>Introduction.....</i>	<i>1</i>
<i>Problems with Building Trust.....</i>	<i>2</i>
<i>Steps to Building Trust.....</i>	<i>7</i>
<i>Conclusion.....</i>	<i>8</i>
<i>References.....</i>	<i>9</i>
<b>Chapter II</b>	
<b>Need for Morality and Ethics.....</b>	<b>10</b>
<i>Introduction.....</i>	<i>10</i>
<i>Morality.....</i>	<i>11</i>
<i>Ethics.....</i>	<i>11</i>
<i>Codes of Professional Responsibility.....</i>	<i>18</i>
<i>The Relevancy of Ethics in Modern Life.....</i>	<i>20</i>
<i>Conclusion.....</i>	<i>21</i>
<i>References.....</i>	<i>21</i>

<b>Chapter III</b>	
<b>Building an Ethical Framework for Decision Making .....</b>	<b>22</b>
<i>Introduction.....</i>	22
<i>Principle of Duty of Care.....</i>	23
<i>Work and Decision Making.....</i>	23
<i>Pillars of a Working Life.....</i>	25
<i>Need for an Ethical Education.....</i>	28
<i>Decision Making and the Ethical Framework.....</i>	35
<i>Conclusion.....</i>	39
<i>References.....</i>	40

<b>Chapter IV</b>	
<b>Security, Anonymity, and Privacy .....</b>	<b>41</b>
<i>Introduction.....</i>	41
<i>Security.....</i>	42
<i>The Importance of Information Security.....</i>	49
<i>Government and International Security Standards.....</i>	50
<i>Information Security Evaluation Criteria.....</i>	53
<i>Privacy.....</i>	56
<i>Privacy and Security in Cyberspace.....</i>	59
<i>Conclusion.....</i>	63
<i>References.....</i>	64

**Section II:  
Security Through Innovative Hardware and Software Systems**

<b>Chapter V</b>	
<b>Software Standards, Reliability, Safety, and Risk .....</b>	<b>66</b>
<i>Introduction.....</i>	66
<i>The Role of Software in the Security of Computing Systems.....</i>	67
<i>Software Standards.....</i>	70
<i>Reliability.....</i>	76
<i>Software Security.....</i>	79
<i>Causes of Software Failures.....</i>	82
<i>Conclusion.....</i>	86
<i>References.....</i>	87

<b>Chapter VI</b>	
<b>Network Basics and Securing the Network Infrastructure.....</b>	<b>88</b>
<i>Introduction.....</i>	88
<i>Computer Network Basics.....</i>	89
<i>Network Protocols and Layering.....</i>	97
<i>Network Services.....</i>	104
<i>Network Connecting Devices.....</i>	108
<i>Securing the Network Infrastructure: Best Practices.....</i>	114
<i>Conclusion.....</i>	118
<i>References.....</i>	118

<b>Chapter VII</b>	
<b>Security Threats and Vulnerabilities.....</b>	<b>119</b>
<i>Introduction.....</i>	119
<i>Types of Threats and Vulnerabilities.....</i>	120
<i>Sources of Information Security Threats.....</i>	122
<i>Best Practices of Online Security.....</i>	133
<i>Conclusion.....</i>	134
<i>References.....</i>	134
<i>Appendix: Additional Reading.....</i>	135
<b>Chapter VIII</b>	
<b>Security Policies and Risk Analysis.....</b>	<b>137</b>
<i>Introduction.....</i>	137
<i>Information Security Policy.....</i>	138
<i>Aspects of Security Policies.....</i>	139
<i>Building a Security Policy.....</i>	142
<i>Types of Security Policies.....</i>	157
<i>Conclusion.....</i>	160
<i>References.....</i>	160
<b>Chapter IX</b>	
<b>Security Analysis, Assessment, and Assurance.....</b>	<b>161</b>
<i>Introduction.....</i>	161
<i>Threat Identification.....</i>	162
<i>Security by Analysis.....</i>	168
<i>Security Assessment and Assurance.....</i>	171
<i>Conclusion.....</i>	179
<i>References.....</i>	179
<b>Chapter X</b>	
<b>Access Control, Authentication, and Authorization.....</b>	<b>180</b>
<i>Introduction.....</i>	180
<i>Definitions.....</i>	181
<i>Access Control.....</i>	181
<i>Authentication.....</i>	191
<i>Authorization.....</i>	203
<i>Conclusion.....</i>	207
<i>References.....</i>	207
<b>Chapter XI</b>	
<b>Perimeter Defense: The Firewall.....</b>	<b>209</b>
<i>Introduction.....</i>	209
<i>Types of Firewalls.....</i>	212
<i>Other Firewalls.....</i>	227
<i>Virtual Private Network.....</i>	230
<i>Firewall Issues Before Installation.....</i>	231
<i>Configuration and Implementation of a Firewall.....</i>	232
<i>Advantages of Firewalls.....</i>	234

<i>Disadvantages of Firewalls</i> .....	235
<i>Securing a Network by a Firewall</i> .....	236
<i>Conclusion</i> .....	237
<i>References</i> .....	238

**Chapter XII**

<b>Intrusion Detection and Prevention Systems</b> .....	<b>239</b>
<i>Introduction</i> .....	239
<i>Definitions</i> .....	240
<i>Background of Intrusion Detection</i> .....	242
<i>Basic Modules of an Intrusion Detection System</i> .....	243
<i>Intrusion Detection Models</i> .....	244
<i>Responses to Intrusion Detection Reports</i> .....	247
<i>Types of Intrusion Detection Systems</i> .....	248
<i>Challenges for Intrusion Detection</i> .....	254
<i>Intrusion Prevention Systems (IPSs)</i> .....	255
<i>Conclusion</i> .....	258
<i>References</i> .....	258

**Chapter XIII**

<b>Security in Wireless Systems</b> .....	<b>259</b>
<i>Introduction</i> .....	259
<i>Types of Wireless Technology</i> .....	260
<i>The Wireless Communication Infrastructure</i> .....	260
<i>Wireless Local Area Network (WLAN): Wireless Fidelity (Wi-Fi)</i> .....	265
<i>Security Issues in Wireless Systems</i> .....	270
<i>Best Practices for Wi-Fi Security</i> .....	276
<i>Conclusion</i> .....	278
<i>References</i> .....	278

**Chapter XIV**

<b>Biometrics for Access Control</b> .....	<b>280</b>
<i>Introduction</i> .....	280
<i>History of Biometrics</i> .....	281
<i>Biometric Authentication System</i> .....	282
<i>Biometric Identifiers</i> .....	284
<i>Advantages of Biometrics</i> .....	292
<i>Disadvantages of Biometrics</i> .....	293
<i>Why Biometrics are Not Truly Accepted</i> .....	294
<i>The Future of Biometrics</i> .....	295
<i>Conclusion</i> .....	296
<i>References</i> .....	296



**Section III:  
Security Through the Legal System**

<b>Chapter XV</b>	
<b>Digital Evidence and Computer Crime.....</b>	<b>298</b>
<i>Introduction.....</i>	298
<i>Definitions.....</i>	299
<i>Nature of Digital Evidence.....</i>	299
<i>Importance of Digital Evidence.....</i>	300
<i>Reliability of Digital Evidence.....</i>	301
<i>The Need for Standardization.....</i>	302
<i>Proposed Standards for the Exchange of Digital Evidence.....</i>	303
<i>The Process of Digital Evidence Acquisition.....</i>	305
<i>Investigative Procedures.....</i>	306
<i>Conclusion.....</i>	316
<i>References.....</i>	316

<b>Chapter XVI</b>	
<b>Digital Crime Investigation and Forensics.....</b>	<b>318</b>
<i>Definition.....</i>	318
<i>Computer Forensics.....</i>	319
<i>History of Computer Forensics.....</i>	319
<i>Network Forensics.....</i>	320
<i>Forensics Analysis.....</i>	321
<i>Forensics Tools.....</i>	324
<i>Conclusion.....</i>	334
<i>References.....</i>	334

**Section IV:  
What Next?**

<b>Chapter XVII</b>	
<b>Trends in Information Assurance.....</b>	<b>336</b>
<i>Introduction.....</i>	336
<i>Global Information Assurance Initiatives and Trends.....</i>	337
<i>National and International Information Security Initiatives.....</i>	342
<i>Certification Programs.....</i>	350
<i>Conclusion.....</i>	352
<i>References.....</i>	353
<i>Appendix: Additional Reading.....</i>	354

<b>Glossary of Terms.....</b>	<b>355</b>
-------------------------------	------------

<b>About the Authors.....</b>	<b>362</b>
-------------------------------	------------

<b>Index.....</b>	<b>363</b>
-------------------	------------