Preface to Third Edition

The second edition of this book came out barely 2 years ago and we are again in need of a new and improved third edition. This rapid turnaround of editions of a successful book like this is indicative of the rapidly changing technology landscape. To keep a promise we made to our readers in the first edition of keeping the book materials as up to date as possible, we have now embarked on this third edition.

First, recall that in the second edition, we introduced to the reader the concept of a changing traditional Computer Network as we knew it when the first edition of this book came out. That network with a nicely “demarcated” and heavily defended perimeter wall and well guarded access points has been going into a transformation as a result of new technologies. Changes have occurred, as we pointed out in the second edition, within and outside the network we call the “traditional computer network”, at the server and most importantly at the boundaries. A virtualized and elastic network with rapid extensions at will is taking its place to meet the growing needs of users. The new technologies driving this change, for now, are system resource virtualization, the evolving cloud computing models and a growing and unpredictable mobile computing technology creating platforms that demand new extensions, on the fly and at will, to the traditional computer network. Secondly, the rapidly merging computing and telecommunication technologies, we started discussing in the first and through the second editions, are rapidly destroying the traditional computer network as mobile and home devices are slowly becoming part of the enterprise and at the same time remaining in their traditional public commons, thus creating unpredictable and un-defendable enterprise and home networks. When you think of a small mobile device now able to connect to a private enterprise network under the BYOD policies and the same device is able to be used as a home network device and at the same time remains connected to networks in public commons, you start to get an image of the “anywhere and everywhere” computing network, a global sprawl of networks within networks and indeed networks on demand. The ubiquitous nature of these new computing networks is creating new and uncharted territories with security nightmares. What is more worrying is that along with the sprawl, we are getting all types of characters joining amass in the new but rapidly changing technological “ecosystem”, for lack of a better word.

For these reasons, we need to remain vigilant with better, if not advanced, computer and information security protocols and best practices because the frequency of
computing and mobile systems attacks and the vulnerability of these systems will likely not decline, rather they are likely to increase. More efforts in developing adaptive and scalable security protocols and best practices and massive awareness, therefore, are needed to meet this growing challenge and bring the public to a level where they can be active and safe participants in the brave new worlds of computing.

This guide is a comprehensive volume touching not only on every major topic in computing and information security and assurance, but also has gone beyond the security of computer networks as we used to know them, to embrace new and more agile mobile systems and new online social networks that are interweaving into our everyday fabric, if not already. We bring into our ongoing discussion on computer Network security, a broader view of the new wireless and mobile systems and online social networks. As with previous editions, it is intended to bring massive security awareness and education to the security realities of our time, a time when billions of people from the remotest place on earth to the most cosmopolitan world cities are using the smartest, smallest, and more powerful mobile devices loaded with the most fascinating and worrisome functionalities ever known to interconnect via a mesh of elastic computing networks. We highlight security issues and concerns in these public commons and private bedrooms the globe over.

The volume is venturing into and exposing all sorts of known security problems, vulnerabilities and the dangers likely to be encountered by the users of these devices. In its own way, it is a pathfinder as it initiates a conversation towards developing better algorithms, protocols, and best practices that will enhance security of systems in the public commons, private and enterprise offices and living rooms and bedrooms where these devices are used. It does this comprehensively in five parts and 25 chapters. Part I gives the reader an understanding of the working and security situation of the traditional computer networks. Part II builds on this knowledge and exposes the reader to the prevailing security situation based on a constant security threat. It surveys several security threats. Part III, the largest, forms the core of the guide and presents to the reader most of the best practices and solutions that are currently in use. Part IV goes beyond the traditional computer network as we used to know it to cover new systems and technologies that have seamlessly and stealthlessly extended the boundaries of the traditional computer network. Systems and technologies like virtualization, cloud computing and mobile systems are introduced and discussed. A new Part V ventures into the last mile as we look at the new security quagmire of the home computing environment and the growing home hotspots. Part VI, the last part, consists of projects.

As usual, in summary, the guide attempts to achieve the following objectives:

- Educate the public about computer security in the traditional computer network.
- Educate the public about the evolving computing ecosystem created by the eroding boundaries between the enterprise network, the home network and the rapidly growing public-commons-based social networks all extending the functionalities of the traditional computer network.
• Alert the public to the magnitude of the vulnerabilities, weaknesses and loopholes inherent in the traditional computer network and now resident in the new computing ecosystem.

• Bring to the public attention effective security solutions and best practice, expert opinions on those solutions, and the possibility of ad hoc solutions

• Look at the roles legislation, regulation, and enforcement play in securing the new computing ecosystem.

• Finally, initiate a debate on developing effective and comprehensive security algorithms, protocols, and best practices for new computing ecosystem.

Since the guide covers a wide variety of security topics, algorithms, solutions, and best practices, it is intended to be both a teaching and a reference tool for those interested in learning about the security of evolving computing ecosystem. Learn about available techniques to prevent attacks on these systems. The depth and thorough discussion and analysis of most of the security issues of the traditional computer network and the extending technologies and systems, together with the discussion of security algorithms, and solutions given, make the guide a unique reference source of ideas for computer network and data security personnel, network security policy makers, and those reading for leisure. In addition, the guide provokes the reader by raising valid legislative, legal, social, technical and ethical security issues, including the increasingly diminishing line between individual privacy and the need for collective and individual security in the new computing ecosystem.

The guide targets college students in computer science, information science, technology studies, library sciences, engineering, and to a lesser extent students in the arts and sciences who are interested in information technology. In addition, students in information management sciences will find the guide particularly helpful. Practitioners, especially those working in data and information-intensive areas, will likewise find the guide a good reference source. It will also be valuable to those interested in any aspect of information security and assurance and those simply wanting to become cyberspace literates.

Book Resources

There are two types of exercises at the end of chapter: easy and quickly workable exercises whose responses can be easily spotted from the proceeding text; and more thought provoking advanced exercises whose responses may require research outside the content of this book. Also Chap. 25 is devoted to lab exercises. There are three types of lab exercises: weekly or bi-weekly assignments that can be done easily with either reading or using readily available software and hardware tools; slightly harder semester-long projects that may require extensive time, collaboration, and some research to finish them successfully; and hard open-research projects that require a lot of thinking, take a lot of time, and require extensive research. Links are provided below for Cryptographic and Mobile security hands-on projects from...
two successful National Science Foundation (NSF) funded workshops at the author’s university.

• Teaching Cryptography Using Hands-on Labs and Case Studies – http://web2.utc.edu/~djy471/cryptography/crypto.htm

We have tried as much as possible, throughout the guide, to use open source software tools. This has two consequences to it: one, it makes the guide affordable keeping in mind the escalating proprietary software prices; and two, it makes the content and related software tools last longer because the content and corresponding exercises and labs are not based on one particular proprietary software tool that can go out anytime.

Instructor Support Materials

As you consider using this book, you may need to know that we have developed materials to help you with your course. The help materials for both instructors and students cover the following areas:

• Syllabus. There is a suggested syllabus for the instructor.
• Instructor PowerPoint slides. These are detailed enough to help the instructor, especially those teaching the course for the first time.
• Answers to selected exercises at the end of each chapter.
• Laboratory. Since network security is a hands-on course, students need to spend a considerable amount of time on scheduled laboratory exercises. The last chapter of the book contains several laboratory exercises and projects. The book resource center contains several more and updates. Also as we stated above, links are also included at the author’s website for Cryptographic hands-on project from two successful National Science Foundation (NSF) funded workshops at the author’s university.

These materials can be found at the publisher’s website at http://www.springer.com/978-1-4471-6653-5 and at the author’s website at http://www.utc.edu/Faculty/Joseph-Kizza/

Chattanooga, TN, USA Joseph Migga Kizza
June, 2014
Guide to Computer Network Security
Kizza, J.M.
2015, XXII, 545 p. 108 illus., 58 illus. in color., Hardcover