At its core, information security deals with the secure and accurate transfer of information. While information security has long been important, it was, perhaps, brought more clearly into mainstream focus with the so-called “Y2K” issue. The Y2K scare was the fear that computer networks and the systems that are controlled or operated by software would fail with the turn of the millennium, since their clocks could lose synchronization by not recognizing a number (instruction) with three zeros. A positive outcome of this scare was the creation of several Computer Emergency Response Teams (CERTs) around the world that now work cooperatively to exchange expertise and information, and to coordinate in case major problems should arise in the modern IT environment.

The terrorist attacks of 11 September 2001 raised security concerns to a new level. The international community responded on at least two fronts; one front being the transfer of reliable information via secure networks and the other being the collection of information about potential terrorists. As a sign of this new emphasis on security, since 2001, all major academic publishers have started technical journals focused on security, and every major communications conference (for example, Globecom and ICC) has organized workshops and sessions on security issues. In addition, the IEEE has created a technical committee on Communication and Information Security.

The first editor was intimately involved with security for the Athens Olympic Games of 2004. These games provided a testing ground for much of the existing security technology. One lesson learned from these games was that security-related technology often cannot be used effectively without violating the legal framework. This problem is discussed – in the context of the Athens Olympics – in the final chapter of this handbook.

In this handbook, we have attempted to emphasize the interplay between communications and the field of information security. Arguably, this is the first time in the security literature that this duality has been recognized in such an integral and explicit manner.

It is important to realize that information security is a large topic – far too large to cover exhaustively within a single volume. Consequently, we cannot claim to provide a complete view of the subject. Instead, we have chosen to include several surveys of some of the most important, interesting, and timely topics, along with a significant number of research-oriented papers. Many of the research papers are very much on the cutting edge of the field.

Specifically, this handbook covers some of the latest advances in fundamentals, cryptography, intrusion detection, access control, networking (including extensive sections on optics and wireless systems), software, forensics, and legal issues. The editors’ intention, with respect to the presentation and sequencing of the chapters, was to create a reasonably natural flow between the various sub-topics.
Finally, we believe this handbook will be useful to researchers and graduate students in academia, as well as being an invaluable resource for university instructors who are searching for new material to cover in their security courses. In addition, the topics in this volume are highly relevant to the real world practice of information security, which should make this book a valuable resource for working IT professionals. In short, we believe that this handbook will be a valuable resource for a diverse audience for many years to come.

Mark Stamp 
Peter Stavroulakis

San Jose 
Chania
Handbook of Information and Communication Security
Stavroulakis, P.; Stamp, M. (Eds.)
2010, XVI, 867 p., Hardcover
ISBN: 978-3-642-04116-7