Information Warfare and Security

by Dorothy E Denning

published by ACM press, in collaboration with Addison Wesley,
ISBN 0-201-43303-6, copyright 1999 by the ACM Press,
list price of $34.95 in the U.S.

reviewed by: H. V. Jagadish,
Dept. of Electrical Engineering and Computer Science,
University of Michigan,
Ann Arbor, MI 48109-2122.
jag@umich.edu

I never thought I would find a technical book that makes pleasant bedtime reading - I was wrong. This book is a joy to read, with page after page of "war stories" the author has collected over the years. (It isn't quite a "you cannot put it down page-turner" like a good mystery novel, but that is only because the average story is less than a page long. And any way, that is asking for too much in a serious piece of non-fiction.)

In terms of content, what blew me away was the staggering scope of subject matter addressed by the author. As a computer-geek, if you asked me to define "information warfare/security" I would talk about the hacking of web-sites, networks, and computers. As a database researcher, my concern is often limited only to database security. Here is a book that places these concerns in context. Information has had value through the ages, and much before the computer was in existence. Consequently, there has always been a role for spies, for disinformation, and for altering records. Modern technology merely provides new avenues to accomplish such tasks.

Fittingly, the bulk of the book is divided into two sections: one on offensive information warfare and one on defensive information warfare. The former describes a wide range of attacks that are possible, ranging from masquerade to eavesdropping to insider betrayal. The latter describes possible defenses to these attacks, along with costs and limitations of these. In particular, it becomes evident that cryptography addresses only a very small part of the larger problem. There is a third section to the book, which actually precedes the two sections mentioned above. In this introductory portion, the author develops a theory of the value of information, and establishes the intellectual framework required for the remainder of the book.

There are swirling political controversies surrounding many information management issues in today's world, ranging from copy protection to unsolicited e-mail. Given the nature of the subject matter in this book, it is hard to describe in a "neutral" way, without taking a political stance. A great strength of this book is that the author, for the most part, is successful in doing this. For instance,

even with regard to offense versus defense in information warfare, the author is value-neutral: not all offense is bad, not all defense is good. Similarly, when discussing the publication by a hacker of a security flaw in a popular piece of software, the author merely presents excerpts from the trial (the prosecution comparing this publication to an announcement that the door to some house is unlocked, and the defense emphasizing the warning to the lock company to build a better lock) and leaves it to the reader to form an opinion on the appropriateness of the hacker's actions.

In conclusion, here is a book that is neither a textbook nor a scholarly reference. Given the enormous breadth of subject matter addressed, it is not able to consider any one issue in sufficient depth to satisfy the reader. Yet, the book is well worth studying, and not just because it is replete with examples, and so a pleasure to read, even for a person with very limited knowledge of computer science. It is a foundational book that defines the scope and proposes a taxonomy for a topic of great importance. It brings structure to otherwise completely inchoate subject matter. And it whets the appetite of the reader to get deeper into the field. In this sense, this book truly advances human knowledge. It both educates the reader and makes one think. It should be required reading for any one who wishes to play a role in defining policies or laws in the light of today's information technology.