Books

Routing in Communications Networks, Martha Streenstrup, Editor, Prentice Hall, Englewood Cliffs, New Jersey, 1995. 399 pp. (ISBN 0-13-010752-2).

Routing in Communications Networks is a book designed for use as a textbook and/or as a reference work. As a textbook, the material is suitable for courses on routing, ranging in level from advanced undergraduate to advanced graduate. As a reference work, it is intended primarily for network researchers, designers, and managers. The organization of this book is excellent and I believe the book will have no difficulty in attracting a much broader audience than those just mentioned.

The book comprises an edited collection of eleven chapters, divided into four parts, written by many of the experts who have contributed to the development of routing protocols in communications networks. It is organized into the following sections: Circuit-Switched Networks, Packet-Switched Networks, High-Speed Networks, and Mobile Networks.

Part I, Circuit-Switched Networks, contains two chapters. Chapter 1 describes dynamic alternative routing, a routing strategy that has been implemented in the British Telecom public switched-trunk network. Chapter 2 is on routing in ATM networks. This chapter describes an innovative approach to ATM virtual-circuit route selection in accordance with users' service requirements. The basic route selection algorithm and its variants are derived from the Least Loaded Routing algorithm.

Part II, Packet-Switched Networks, contains four chapters. Chapter 3 describes distance-vector routing, which served as the basis for the Internet. Chapter 4 covers three inter-domain routing protocols: the Exterior Gateway Protocol (EGP), the Border Gateway Protocol (BGP), and the Inter-Domain Routing Protocol (IDRP), which are used in heterogeneous internets comprising multiple organizations. Chapter 5 covers link-state routing. Link-state routing information distribution, route generation techniques, and several examples of internetwork routing procedures are presented. The final chapter discusses AppleTalk**, a specific routing mechanism designed as a commercial product. This chapter describes the protocols that constitute AppleTalk and offers some insight into its development.

Part III, High-Speed Networks, contains three chapters: Chapter 7—"Routing in Optical Networks," Chapter 8—"Routing in the plaNET Network," and Chapter 9—"Deflection Routing." These chapters reflect the variety of today's high-speed networking technologies and associated routing strategies. Each of these chapters contains an up-to-date and complete bibliography that contains references to seminal works in each of these areas.

Part IV, Mobile Networks, contains the final two chapters. Chapter 10, "Routing in Cellular Mobile Radio Communications Networks," is an excellent introduction to cellular communications. It covers system basics, architectures, and standards. The final chapter, "Packet-Radio Routing," addresses routing strategies for packet-radio networks.

Each of the sections of this book is self-contained and can be read without reading the other sections. Although each chapter of the book was written by different authors, I must admit that I was surprised by the consistency of each chapter. The editor did a terrific job of blending together the various topics. Each section contains an overview that relates

the chapters contained in that section and each chapter begins with a short abstract outlining the contents of the chapter. In short, the book is very well organized!

An appropriate tone was consistently maintained throughout the book. I found the chapter, "Routing in Optical Networks," of particular interest. It provided a clear discussion of the technologies involved and gave a natural framework within which to discuss routing. This was the best description and overview of optical networks I have read to-date. The 74 references provided at the end of the chapter were accurate, complete, and appropriate as well.

In summary, this book is a very good introductory-level textbook. It covers, in sufficient detail, many of the routing techniques in use today. I highly recommend this book for anyone who is interested in understanding the similarities and differences among the various routing techniques in use today and the reasons for many of the design choices that were made during their development. It is nice to have a reference containing many of the routing strategies currently employed in communications networks all contained in one book.

Ronald J. Vetter
Department of Computer Science
North Dakota State University
Fargo
North Dakota

**Trademark or registered trademark of Apple Computer, Inc.

Network Security: Private Communication in a Public World, Charlie Kaufman, Radia Perlman, and Mike Speciner, Prentice Hall, Englewood Cliffs, New Jersey, 1995. 504 pp. (ISBN 0-13-061466-1).

Cryptography has been the province of governments and spies for most of history. Relatively recently, financial institutions have used cryptography to protect information associated with an electronic funds transfer (EFT) and to secure a customer's personal identification number (PIN) entered into an automated teller machine (ATM). Today, with the increasing use of networking and the Internet, we see the emergence of serious cryptography as a tool for all people, providing secure electronic mail capability with confidentiality (that is, assurance that a note is revealed only to those intended), integrity (that is, assurance that a note is as intended), and nonrepudiation (that is, assurance that a note is from the claimed sender and that this can be demonstrated to an impartial third party).

This book is a welcome addition to the evolving corpus of current methods used to achieve security in a network and on the Internet. The authors' stated goal was to write a book on computer security readable by a novice, yet containing technical depth. In this, they succeed. Many insightful attack scenarios are included, especially in security protocols, and for this reason alone *Network Security* should be on the bookshelf of every security designer. This is a book that is meant to be practical and meant to be used. Furthermore, I found this book witty and fun to read, with appropriate humorous quotes and wry examples to enliven most subjects. For example, a broadcast scenario uses Bob and Carol and Ted and Alice arranging to get together at Alice's apartment.

The book is organized into major sections entitled Cryptography, Authentication, Electronic Mail, and Leftovers. It may be used as a graduate textbook, containing homework problems of varying difficulty at the end of each chapter. Do not overlook these if you are trying to get the most out of this book. The questions are thoughtful, asking the reader to ferret out conceptual mistakes and security flaws in hypothetical scenarios.

The Data Encryption Standard (DES) and the International Data Encryption Algorithm (IDEA) are two secret key algorithms described. The ways they are used to provide data confidentiality and data integrity are given.

The public key algorithms discussed are the Rivest-Shamir-Adleman (RSA) algorithm for digital signature and secret key transport, the Diffie-Hellman algorithm for secret key agreement, and the Digital Signature Standard (DSS) from the National Institute of Standards and Technology (NIST). The orientation of the description of the first two algorithms is based on the Public Key Cryptography Standards (PKCS) published by RSA Data Security, Inc., and many attacks thwarted by the PKCS design are described. One-way hash functions covered are the Message Digest algorithms from the PKCS (MD2, MD4, and MD5) and NIST's Secure Hash Algorithm Revision 1 (SHA-1), as well as many

uses for such functions. There is also a section on number theory as it pertains to the mathematics of cryptographic algorithms, which can be skipped if one does not need to know the details of the arithmetic.

I suppose there must be a cut-off point when deciding what to include, but I hope a future edition will cover some of the existing and emerging standards developed by the International Organization for Standardization (ISO), the American National Standards Institute (ANSI), and European efforts. For example, the ISO 9796 standard specifies the use of the RSA algorithm with a special formatting process to address certain security concerns, and the ISO 10118 suite of hash function standards includes the MDC-2 and RIPE-MD hash functions. As the global information infrastructure becomes more dependant on cryptography, it seems prudent to many people to have suites of algorithms based on differing principles, so that the unexpected breaking of any one allows for rapid substitution.

In the section on authentication, the authors describe the basic problem of entity authentication and give examples from simple password methods to the advanced ticket-granting schemes of Kerberos Version 4 and Kerberos Version 5. Along the way they describe many pitfalls to look out for in designing an authentication system.

Electronic mail security is covered, including discussions on the Internet Engineering Task Force (IETF) Privacy Enhanced Mail (PEM) standards, Phil Zimmermann's Pretty Good Privacy (PGP) "guerrilla freeware," and the CCITT X.400 suite of standards. As they note, it is somewhat surprising that these three solutions to approximately the same problem are so different. After describing each method, there is an especially valuable chapter comparing and contrasting these three solutions. In this section, their description of how to use public keys to achieve plausible deniability (that is, send a message so that the receiver knows it is from you but cannot prove it to anyone else) is an interesting twist on the theme of nonrepudiation.

In the section on "leftovers," we find descriptions of the security in Novell's NetWare** Version 3 and NetWare Version 4, IBM's NetSP* Krypto-Knight, Simple Network Management Protocol (SNMP), Digital Equipment Corp.'s Distributed Authentication Security Service (DASS/SPX), Lotus Notes**, the Open Software Foundation's Distributed Computing Environment (DCE**), and Microsoft security.

Overall, this book is a very useful compilation of cryptographic insight and analysis of the security of many current products. When compared and contrasted with other recent books on cryptography (for example, *Applied Cryptography* by Bruce Schneier or *Computer Communications Security* by Warwick Ford) it is surprising that, considering they are covering approximately the same subject, they are so different and complementary.

Don B. Johnson
IBM Cryptography Center of Competence
Poughkeepsie
New York

*Trademark or registered trademark of International Business Machines Corporation.

**Trademark or registered trademark of Novell, Inc., Lotus Development Corp., or Open Software Foundation.

Note—The books reviewed are those the Editor thinks might be of interest to our readers. The reviews express the opinions of the reviewers.