TER Volume 4, Issue 10, November 1997

ter

telecommunications electronic reviews

Volume 4, Issue 10, November 1997

Contents:

ter issues (/lita/publications/archive/ter)

REVIEW OF: Walter H.W. Tuttlebee, ed. Cordless Telecommunications Worldwide: the Evolution of Unlicensed PCS. London, UK: Springer-Verlag, 1997.

by Pamela Czapla

An effort by UK Engineering Series editor Nicholas Pinfield to persuade Tuttlebee to update Cordless Telecommunications in Europe grew into the recognition that cordless telecommunications had outgrown its European genesis to become a global industry. Thus writers were solicited from Europe, Asia, and the United States to provide this worldwide perspective on the state-of-the-art.

A word about these writers. In several instances they were the key players in the areas about which they write. The chapter on the Personal Communications Interface (PCI) standard, for example, is written by the editor for the development of that standard, Gary Boudreau. Heinz Ochsner, who writes the chapter on cordless standards in Europe, chaired the committee which developed the Digital Enhanced Cordless Telecommunications (DECT) standard. The chapter on cordless terminal mobility is written by the manager of the cordless terminal mobility project, Graham Crisp.

As Tuttlebee explains in the introduction, this book has dual thrusts. Its intended audience is industry practitioners as well as engineering and business students. Thus the "Markets and Applications" section provides the commercial background. The balance of the book undertakes explanation of the areas of standards and technology. An added bonus is commentary on regulatory and policy environments.

The book features four sections: markets, industrial development, technology, and technical standards. "Markets and Applications" covers European and Asian markets as well as applications such as PBX (Private Branch Exchange), cordless telephone and radio, and cordless local loop. "Standardization and Industry Development" includes separate chapters on Europe, Asia, and the United States, as well as a chapter discussing development and products worldwide.

In "Technology" separate chapters examine audio, radio, cordless networks, cordless data, handsets, and future developments. "Technical Standards" covered are Common Air Interface (CT2), PCI, DECT, Personal Wireless Telecommunications, North American Personal Access Communications System - Unlicensed B (PACS-UB), Personal Handyphone System, Personal Access Communication System - Unlicensed Version A (PACS-US), Orthogonal Code-Division Multiple Access Wireless User Premises Equipment, and Combined Code-Division Multiple Access/Time-Division Multiple Access (CCT). Tables, photos, and 153 figures supplement the text.

The chapters on the technical standards are not for the faint of heart or uninterested. They are, however, quite readable considering the subject matter. The authors provide history and background on the development of individual standards, place each standard in relation to other standards, and discuss rationales behind their development.

This resource is timely, comprehensive, well documented, and delightfully lucid. The hefty price tag will put it out of range of most pocketbooks. Its purchase, however, does buy a compilation of well-documented chapters. The subject matter is examined from a plethora of angles. This book represents an extraordinary coordination effort in bringing together the expertise of these writers. Moreover, cross references are made across chapters so as to further tie together the material. This treatment should be equally valuable to the neophyte and the well- informed.

Those studying wireless communications on a global basis might also want to consider two other recent publications. Rachael E. Schwartz has developed case studies from the standpoint of telecommunications regulators. [1] <reviewed in TER 4(3) (/lita/publications/archive/ter/4/terv4n3april#schwartz)> Brian J. W. Regli addresses "how to use wireless access as a tool to further competition and sustainable development in the telecommunications sector." (p. vii) [2] He writes for managers in public and private sectors and also provides a global perspective.

Notes:

[1] Schwartz, Rachael. (1996). Wireless Communications in Developing Countries: Cellular and Satellite Systems. Boston, MA: Artech House.

[2] Regli, Brian J. W. (1997). Wireless: Strategically Liberalizing the Telecommunications Market. Mahweh, NJ: Lawrence Erlbaum Associates.

Dr. Pamela Czapla (pjc2@psu.edu (mailto:pjc2@psu.edu)) is the Director of the National Cable Television Center Library at Pennsylvania State University.

table of contents ter issues (/lita/publications/archive/ter)

REVIEW OF: Warwick Ford and Michael S. Baum. Secure Electronic Commerce. Englewood Cliffs, NJ: Prentice-Hall, 1997.

by Ray Olszewski

The collection of protocols used on today's Internet (TCP/IP (Transmission Control Protocol/Internet Protocol), UDP (User Datagram Protocol), and services such as Telnet, FTP (File Transmission Protocol), HTTP (Hypertext Transfer Protocol), and SMTP (Simple Mail Transfer Protocol)) constitute the lingua franca of modern, large-scale computer networking. But these protocols originated on a smaller, clubbier Internet, one where participants largely knew and trusted one another. As Internet use exploded in recent years, and especially as it came to be seen as a system for transacting everyday business, deficiencies in the Internet protocol suite became increasingly apparent.

Making the Internet secure for transacting business has three main components:

Authentication: For an individual user, this means making sure that the site they connect to is the site that it says it is. For a site providing services, it means making sure that individuals who connect to the site are who they say they are. This matters for electronic ordering ("Who am I giving my credit card number to?"), delivering commercial and shareware programs via networks ("Is it real or is it a Trojan horse?"), and acceptance of orders ("Is this credit card stolen?"). It matters as well for providing access to commercially valuable data. Technologies now exist to authenticate Web sites, individuals using Web browsers, email messages, and remote logins via Telnet. Generally, this component involves systems for adding digital signatures, including the procedures for creating "certificate authorities" to verify signatures.

Signature: This includes providing a way to sign an electronic document that is the legal and practical equivalent of signing a contract or other binding agreement. This function simultaneously confirms one's acceptance of its terms and prevents subsequent changes to the document. This component is similar to authentication, but its requirements are somewhat stronger: the mechanism needs to meet legal standards for indicating acceptance of an agreement; the encryption methods used need to be secure for many years

into the future; and signature verification systems need to keep records long enough to be able to verify signatures long after the document is signed. While the technologies used are very similar to authentication, the institutional mechanisms are more elaborate.

Privacy: This component provides a mechanism to prevent eavesdropping on electronic communications. Privacy is needed to protect against interception of credit card numbers and commercially valuable information, as well as protecting transmissions against insertions of fraudulent data. This component involves procedures to encrypt messages, including email, Telnet, and transmission to and from Web servers.

Secure Electronic Commerce is an overview of the technical, legal, and institutional (policies and practices) issues involved in transforming the Internet from an insecure method of communication and interaction to one suitable for conducting large and small business transactions. The authors, a technologist and an attorney, are well placed to perform this review. Both work for VeriSign Inc., a major player in the digital signature business, and Baum has played a central role in creating the policies and practices used by the digital signature industry.

The book is at its best when it focuses on the actual methods being used today to provide authentication, signature, and privacy. The concept of "trusted agent" plays a key role in making security work--basically, in order to use security tools on an open network, you need someone trustworthy to vouch for identities. Authorities like VeriSign use the tools of encryption to provide electronic documents called certificates that provide this "vouch for" function. It sounds simple, but making it work requires enormous attention to detail, and Secure Electronic Commerce is superb at providing the detail needed to flesh out this seemingly simple observation.

Making security work largely involves having a knack for seeing all the ways it can fail, then preventing them one by one. Ford and Baum are experts, if not paranoids, at this kind of analysis, making their extended descriptions of what can go wrong and how to anticipate and avoid it an excellent examination of the workings of Internet security. Their particular strength is on the policies and practices side, where they describe the many ways in which identities, communications channels, and signatures might be compromised, even assuming effective technologies are available. The authors spell out the institutional arrangements needed to make effective use of the technologies to provide security, including steps needed to make digital signatures to documents legally enforceable. In this area, they cover every scenario I have previously encountered or thought of and many that were new to me.

To make all of this understandable, Secure Electronic Commerce also provides overviews of the current state of encryption technology and legal standards. The book's overview of the technologies of encryption and signing is good, identifying and providing nontechnical descriptions of the best known techniques and actual products. While the book emphasizes use of DES-based (Data Encryption Standard) and RSA-based (Rivest, Shamir, Adleman Public Key Encryption) methods, it also includes coverage of other technologies, such as Diffie-Hellman and elliptic-curve public-key systems. But to an expert in this area, it is clear that the book is limited to an overview, offering little in the way of technical insights into the underlying mathematics or programming of encryption. Readers looking for that level of detail would do better to consult an encryption text, such as Schneier's Applied Cryptography, or experiment with the implementations of many encryption algorithms that are freely available in common programming languages. [1]

In contrast to the technology side, legal expertise is not my area. To my eye, the legal overview was a good introduction to the issues involved in doing business electronically, certainly good enough to let me see how the policies and practices that have developed address legal issues. Still, I suspect that an attorney would

offer the same caution here as I did after reading the section on technologies: don't think that reading this section makes you an expert on the legal issues involved.

The book does have its limitations. Both authors are committed to the use of established "Certificate Authorities" along the lines of the VeriSign model, and they tend to dismiss decentralized "vouching for" models of the sort popularized by the Pretty Good Privacy (PGP) system for signing email and files. This model relies on multiple verification and permits a user to begin with one or a few personally known sources, then extend a "circle of trust" outward from them. The approach certainly has its problems, but to my eye, the authors spend too little time considering how decentralized models might be made to work effectively.

Another limitation of the book is the paucity of real-world examples. Stylized cases, used here as in other texts on electronic security, are helpful for illuminating the technical issues, but they leave one uncertain about the economics of providing electronic security. All too often, the methods described seem appropriate for large-dollar contracts, agreements of the sort where electronic communication remains likely to be supplemented by a printed agreement for some time. The costs of security are very real--in fees to certificate authorities, in more expensive server software, in time and bandwidth consumed by encryption, and in setting up and running systems for key management and distribution. These costs need to be weighed against concrete benefits, not fanciful ones imagined in hypothetical examples.

Small-dollar transactions, such as credit card purchases, are likely to emerge as a big part of electronic commerce and an important use of these security systems. In this context, it is striking that the authors do not discuss what Internet security developers might learn from present institutional methods for dealing with authentication and signature in telephone purchases using credit cards. Such transactions have been common for many years, and the credit card and mail-order industries have found ways to adapt to many of the same problems that arise in transacting business over the Internet. Some discussion of how security problems have been addressed in this historical context would have helped the reader assess the practicality of ideas for how to secure transactions over the Internet.

Finally, the authors are a bit too willing to motivate interest in security by providing the standard litany of Internet horror stories. Bad things certainly happen on the Internet, and the authors include the standard list in their introduction, but the connections between these stories and the security systems they describe is often weak. While adding security systems for valuable transactions will protect those transactions against interception, they will not address attacks like the Internet Worm (described on page 4) or more modern approaches to attacking system operation (such as the "denial of service" attack that I suffered through, in which a concealed source floods a site with packets, overloading its hosts and routers). To protect the Internet against these and other kinds of attacks--or at least to make it possible to identify the perpetrators--requires that a system of authenticating packets and messages come into use not merely for high-value communications but for all communications.

While these limitations are real, they should not divert attention from the book's enormous strengths. Classics are rare in the field of computers--things simply change too fast--but Secure Electronic Commerce nonetheless has the makings of a classic, a solid treatment of the institutional issues that any technology for Internet security will have to confront.

Notes:

[1] Schneier, Bruce. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. New York: Wiley.

Ray Olszewski (ray@comarre.com (mailto:ray@comarre.com)) is a consultant specializing in quantitative analysis in Palo Alto, CA.

table of contents ter issues (/lita/publications/archive/ter)

REVIEW OF: Elizabeth Thomsen, ed. Reference and Collection Development on the Internet: A How-to-do-it Manual. New York: Neal-Schuman Publishers, 1996.

by Wendy Wu

Getting to the point of deploying Internet resources consistently at work is difficult, as the Internet has an inherently chaotic and volatile nature and is getting more complicated daily. Librarians, especially those in public libraries who may have limited access to the Internet, are challenged to use different tools to find needed information in cyberspace quickly and to use their professional training and skills to organize the available resources from an identifiable and authoritative point of view. This book has been designed particularly for those librarians to give them a sense of the Internet as a community of individuals and organizations who share information through discussion and newsgroups and online resources.

The book, which is composed of eight chapters, two appendices, and an index, focuses on the Internet as a communication tool and as a dynamic resource that is new and evolving and reflects its populist nature. Since reference and collection development are inevitably transformed by the Internet, librarians must use the Internet to assist their work and professional development.

Chapters one and two of the book introduce the history of the Internet and overview Internet basic tools that everyone should know as they start to surf the Internet. The author gives easy-to-understand descriptions of the origin of the Internet and onlines services such as America Online, Prodigy, Compuserve, and bulletin board systems that have given us a whole new way to form associations and communities of interest. Though the best metaphor for the Internet is perhaps the electronic watering hole, overloaded with sources of information, its primary benefit for most people is electronic communication.

The Internet is not a system or a product or a service provided by vendors that librarians know how to deal with; it is much more complex and based on distributed processing. In chapter two, the author discusses the basic Internet protocols, i.e., email, Telnet, File Transfer Protocol (FTP); how to use three essential services, i.e., participating in training, reading documentation, getting support from the local system administrator; as well as how to get connected to the Internet. WAIS (Wide Area Information System), the uniform resource locator (URL), and client software issues are also covered briefly in this chapter.

Chapters three through eight discuss how reference and collection development librarians can use Internet fundamentals (Listserv, Usenet, Gopher, and World Wide Web) and special resources (library catalogs, databases, electronic books, and Frequently Asked Question (FAQ) files) to enhance their work and offer new services.

Chapters three and four intensively focus on mailing lists (Listserv) and newsgroups (Usenet), how they work, and how to use them professionally. Mailing lists, the oldest social institution on the Internet, have various styles, tones, and contents, but they bring people together to share information and knowledge and to communicate with each other. Librarians will learn from this book the features of mailing lists, how to subscribe to them, how to request the needed information, and how to search archived lists. Several examples of mailing lists devoted to various aspects of librarianship, such as STUMPERS, PACS-L, and PUBLIB, illustrate how to use various subject-oriented groups as a reference or collection development tool. New mailing lists may occur daily, however; thus the author suggests several places to find newly-created lists: looking at books, the new-list available through USENET as bit.listserv.new-list, and online directories.

Usenet is the world's largest bulletin board system covering thousands of different subjects. The author reviews what Usenet is, its hierarchies, technical details, how to use a newsreader (e.g. tin) to read messages, how to get Usenet access, and how to use it to seek needed information. Usenet resources for librarians, especially public librarians, are also listed and discussed in chapter four, which serves as a good starting place for beginners. Quite a few mailing list resources are available through Usenet. In chapter five, the author emphasizes one newsgroup (rec.arts.books) as a very good source on the Internet for reference and collection development.

FAQs developed based on mailing lists or Usenet resources are also helpful for people jumping in on a discussion group; they are also valuable for librarians in answering individual questions. The FAQs have become an important part of Usenet culture and a certain standard format has evolved. FAQs may also have considerable lists of other resources, like subject-oriented guides to the Internet, lists of organizations, newsletters, catalogs, and stores. Chapter six covers how FAQs are posted, their anatomy, how to find the FAQs, and how librarians use FAQs to help people locate information.

In addition to the basic Internet tools discussed above, librarians should also learn how to use World Wide Web (WWW) browsers to access and browse information. In chapter seven, the author gives an overview of Gopher and its history as well as addressing the WWW--browsers, home pages, Hypertext Markup Language, WWW resources, and how to search Internet resources through WWW search engines.

The WWW provides easy access to Telnet and FTP sites, Usenet and FAQs, graphics, databases, and other types of materials available on the Internet. It creates a new form of publishing and a new way for all types of organizations, businesses, and individuals to create and distribute information resources. Therefore, librarians should understand and be a part of this world. Reference librarians in particular need to look for answers to questions posted by patrons through searching or browsing Internet resources. Lycos, one of the earliest Internet search engines, is taken as an example to illustrate how to conduct a subject search on the Web. Collection development librarians may also use the Web to locate book lists or readers' advisory or other information to assist their work.

Chapter eight teaches librarians and patrons how to use library online catalogs all over the world, access databases, and use electronic books, journal, and documents. Examples given are useful and interesting, such as the United State Postal Service (http://www.usps.gov/ncsc/lookups/lookup_zip+4.html) (http://www.usps.gov/ncsc/lookups/lookup_zip+4.html), U.S. Gazetteer (http://tiger.census.gov/cgi-bin/gazetteer (http://tiger.census.gov/cgi-bin/gazetteer)), the e-text project named Bartleby the Scrivener (http://www.columbia.edu/acis/bartleby/index.html (http://www.columbia.edu/acis/bartleby/index.html)) sponsored by Columbia University and created by the Bartleby Library, and a Shakespeare home page (http://the-tech.mit.edu/Shakespeare/search.html (http://the-tech.mit.edu/Shakespeare/search.html)) created by Jeremy Hylton. In a rapidly changing environment, librarians need the skills that allow them to deal with a proliferation of information in all formats.

The third part of the book is composed of two appendices. The first one, the Virtual Vertical File, compiles selectively the Web sources which help reference librarians jump onto the information superhighway quickly. The second one, the List of Lists, selectively organizes useful resources by subject for all librarians to help them serve the community better and more efficiently.

This easy-to-understand book covers all basic aspects of the Internet with good metaphors and detailed discussion. Most of the chapters include examples relevant to librarians' and patrons' interests. It is a very good manual for entry level librarians who have little Internet experience and knowledge and may serve as a practical guide for using the Internet to assist reference services and collection development in the real world.

The book would have been more useful, however, if it had covered more new Internet development. Some content is out of date (e.g., WAIS and Gopher). Due to the Internet's nature, some of the URLs listed in the book are no longer valid.

Wendy Wu (wendywu@med.wayne.edu (mailto:wendywu@med.wayne.edu)) is Information Services Librarian at the Shiffman Medical Library of Wayne State University.

table of contents ter issues (/lita/publications/archive/ter)

About TER