Review of *Secure communications* by R. J. Sutton

(Wiley, 2002)

Chris Mitchell

17th September 2002

Overall this is a somewhat disappointing book. However, this reaction is partly conditioned by the fact that the contents do not live up to the title. There is no way that this book attempts to provide a comprehensive coverage of secure communications. The preface gives the first hint about the real focus, by stating the book is about secure telecommunications. Reading the contents list makes it immediately clear that there are many topics missing that one would expect in any book with this title – for example, there is no significant coverage of Internet security (apart from a very few pages in chapter 12 on VPN security). This is rather regrettable since the IP protocol and its security are of ever increasing importance in the telecommunications world.

A second and more careful reading of the contents list reveal the coverage to be idiosyncratic in the extreme. The book starts with the obligatory couple of introductory chapters – these already ring alarm bells since, judging by the title of chapter 2, the author seems to think digital signatures are a kind of encryption. (This turns out to be symptomatic of an obsession with the importance of encryption over other types of cryptographic technique). The next two chapters deal with voice security or, more precisely, voice encryption. This is followed by a chapter on GSM security. Despite claims in various places in the book that security is about more than encryption, it is not clear that the author really believes this statement, since the

emphasis in this chapter and elsewhere is very much on data encryption. The authentication of GSM mobiles to the base station is a topic hardly mentioned, despite the fact that it is arguable that this security feature is much more important than air interface encryption. This thesis is supported by the fact that, in some countries (e.g. France), GSM networks were originally (successfully) deployed without any air interface encryption. Whilst GSM without encryption therefore appears to be a viable, albeit perhaps undesirable, option, the level of fraud to which the first generation mobile networks were prone suggests that GSM without mobile authentication would simply not be conceivable.

There follows a series of chapters on security in private radio networks, frequency hopping, bulk encryption and fax security. The common approach of these chapters, and also the two earlier chapters on voice encryption and two later chapters on secure VPNs and military data communications, is that of a series of design studies. These studies are presumably based on personal design experience, and describe just one approach to each problem rather than exploring a variety of different design approaches. This is interesting material nevertheless, although it could only be used as tutorial material with great care, since it makes no pretence to scientific objectivity.

Apart from the chapters already mentioned, there are chapters on PC security, secure e-mail, and security management. However, these are also very idiosyncratic in their coverage. For example, the chapter on PC security does not attempt to describe what a virus is, and gives no general discussion of malicious code.

There are other surprising omissions from the book. For example, chapter 11 (on secure e-mail) makes no mention of any of S-MIME, PEM, X.400 or Open-PGP. Nowhere in the book (that I can find) is there any discussion of public key certificates or PKIs. The chapter on security management is pitifully brief, and manages to avoid

any mention of ISO/IEC 17799. The bibliography is very weak indeed; there are a number of major relevant books that are not mentioned.

In conclusion, this book has some merit in being generally well written and accessible, and it also covers topics (notably those relating to military encryption) that are not well covered in other sources. However it has some very serious omissions, and cannot be recommended as a first (or even second) book to buy on the topic of secure communications; even where topics are covered, the reader should not believe that the coverage is in any way a comprehensive treatment. This book will primarily be of interest and value to the specialist, rather than the reader looking for a general introduction to the subject.