is not fulfilling the expectations of users. Similarly while some do not approve of government's active role in development of standards and would prefer the SDOs, and consortia to perform this task, others argue that government should not only play an active role but also provide leadership to the process. These conflicting views are not unique to the US. Rather they reflect the growing importance of Transnational Corporations (TNCs) at the international level. For instance, many TNCs are actively involved in supplying, building and managing telecommunication infrastructures. Similarly in the IT industry, global players dominate the market. One has to understand the controversies in development of standards in this context. Again, the example of Europe, where the European Telecommunication Standards Institute (ETSI), which played a major role in development of European telecommunication standards indicates that the standardization process, how ever complicated and complex it may be, is essential for maintaining competitive advantage.

It has been pointed out that TNCs and consortia are actively involved in tasks relating to standardization, which was once reserved for governments and international agencies.[1] With the signing of global accords under the World Trade Organisation (WTO) for liberalisation of telecommunication services and IT products, this process will gain momentum. With the rapid convergence of computers and communication technologies, the development of standards will become a key area for co-operation as well as conflict. This volume helps the reader to understand the various dimensions of this issue and the views of various actors involved in this question. Although most of the contributions are from the US and deal with questions specific to the US, it is relevant for readers elsewhere also as the debates in the US are too important to be ignored. The vision of NII in the US provides inspiration for similar initiatives elsewhere also and so this book is an important contribution to this topic.

Had there been any contribution from organisations like EFF (Electronic Frontier Foundation) or CPSR (Computer Professionals For Social Responsibility) it would have been better. Still this does not reduce the importance of this volume for readers and policy makers, who are dealing with the development of Information Infrastructure and standards.

Notes and References

1. A.M. Rutkowski, 'Multilateral Cooperation in Telecommunications', in William J. Drake (ed.), *The National Information Infrastructure: Strategies for US Policy*, The Twentieth Century Fund, New York, 1995.

K. Ravi Srinivas
Madurai
India

Information Security—The Next Decade

Jan H.P. Eloff & Sebastian H. von Solms (Eds)

London, Chapman & Hall, 1995, viii + 625 pp., UK £69.00, ISBN 0 412 64020 1

This volume is subtitled *Proceedings of the IFIP TC 11 eleventh international conference on information security, IFIP/Sec '95.* It contains 45 papers arranged in 12 parts on the following themes: Information Security and Business Applications, Information Security Standards, Management of Information Security Cryptography, Key Management Schemes and Mobile Computing; Information Security and Groupware; Building Secure Applications; Open Distributed Security; Access Control; and Legal, Ethical and Social Issues of Information Security. Each part contains generally three to five papers. Three

of the themes have two parts devoted to them: Information Security and Business Applications; Management of Information Security; and Open Distributed Security.

The breadth of the material presented illustrates the expanding relevance of security-related issues in an increasingly complex world. At a time when the Internet is achieving increasing acceptance and raising some new questions, when some argue that international borders are no longer relevant, when the strategic relocation of transnational corporations require greater use of secure communication channels, it is perhaps inevitable that security should require a multi-disciplinary approach. The topics examined here illustrate this variety: medical database systems, financial systems, encryption policy, risk assessment, mobile computing, groupware, authentication services, digital signatures, smart card applications, and ethics. At a time of significant change, the emergence of new technologies continues to raise new questions and increase the need for new methods.

Five of the contributions are invited talks: W. H. Murray, 'Security should pay: it should not cost'; L. J. Hoffman, 'Encryption policy for the Global Information Infrastructure'; D. B. Parker. 'A new framework for information security to avoid information anarchy'; S. Muftic 'Functional and operational security system for open distributed environments'; and F. B. Cohen, 'Viruses, corruption, denial, disruption and information assurance'.

Hoffman gives a lucid summary of some of the legal and political issues involved including law enforcement, export controls and civil liberties. Many of the issues resulted from recent US government policy on encryption and its attempts to tightly control the export of secure encryption methods, highlighted by the introduction of the Clipper chip and subsequent heated discussion. The futility of some of the methods employed by the government is most vividly shown by the decision of one US group to base its operations outside the US in order to maximise its export markets (including the US). Perhaps international borders are not quite irrelevant just yet, so long as they have a bearing on legal jurisdiction.

Donn Parker argues convincingly against the widely-held view that information security deals only with preserving confidentiality, integrity and availability of information and that authenticity, utility and possession of information must also be considered. He cautions that future developments may require the addition of further elements. His view is supported by a series of illustrative loss scenarios.

Cohen details some of the history of viruses, some standard data protection methods and questions some of the anomalies of data security, in particular the failure to adopt superior methods which are widely available, in some case at lower cost than current methods. He also draws attention to some of the cause of security problems, including 'The universities of the world have, with a few notable exceptions, provided inadequate education in the information assurance area ...'.

Adrian Warman in 'Developing policies, Procedures and Information Security Systems' deals with some of the issues involved in developing policies and procedures and examines their effectiveness in current implementation. Some of the conclusions are likely to be of considerable use to organisations in developing their own policies and should enable them to benefit from the experiences of others.

J. H. Carroll's 'Portrait of the Computer Criminal' gives an interesting insight into the history of computer-related crime and explores some of the methods used. It deals with the computer as both object of crime and tool of crime. The author's enthusiasm for the subject, while admirable, occasionally leads to sweeping generalisation such as the arguable 'In the 21st century almost all crime against property will be perpetrated within computer systems'.

Anja Hartmann in 'Comprehensive Information Technology Security: A new Approach to Respond Ethical and Social Issues Surrounding Information Security in the 21st century' seeks to take a wider view of IT security with emphasis on the ethical and social as opposed to the organisational, technical and legal questions which have tended to dominate. This discussion is novel and timely but it also illustrates some of the problems in ethical considerations. Wrestling with questions of responsibility and conscience are fraught with difficulty and the subject of much unresolved debate among philosophers. The discussion also appears to overlook the fact that for some people ethical considerations are neither incentive nor obstacle. The consequences of such views also need to be considered.

This volume is certain to appeal to those with an interest in information security generally and, in particular, anyone who wishes to examine in detail the material presented at the IFIP TC11 conference. As might be expected some of the material is quite specialised and is unlikely to attract the reader who doesn't have a substantial background in the relevant area. This is the case in particular with parts four and eleven (Cryptography, Key Management Schemes and Mobile Computing; Access Control).

In part four, for example, G. Carter *et al.* in 'Analysis of DES Double Key Mode' describe a detailed cryptanalysis of a new mode of Data Encryption Standard (DES) which allows a 112-bit key, based on doubts raised during the early 1990s about the security of the DES algorithm.

One of the more recent developments in authentication is explored by W. G. de Ru and J. H. P. Eloff in 'Reinforcing password authentication with typing biometrics'. The analysis of a user's keystroke patterns is used to augment conventional authentication mechanisms. The authors argue that fuzzy logic techniques based on typing biometrics offer improved security at comparatively modest additional cost. This approach appears to offer some significant advantages including a reduced risk of damage from a compromised password, the inability to copy a user's biometrics profile by observing typing, easy integration into current systems, etc.

This book has something to offer any reader with more than a casual interest in information security, including the specialist. For the non-specialist, it provides an insight into those areas which were attracting considerable research effort during the early and mid 1990s, with many suggestions for future research directions.

If there is a problem with this book, it is the print quality. The quality varies, and while some of it is of a high standard, much of the text is faint and in a font size which is too small to make it comfortable to read. It is a pity that such a shortcoming, which could probably have been easily rectified, detracts from the material presented.

David Colhoun
University of Wollongong
Wollongong, Australia

Institutional and Entrepreneurial Leadership in the Brazilian Science and Technology Sector—Setting a New Agenda, World Bank Discussion Paper No. 325

Lauritz Holm-Nielsen, Michael Crawford & Alcyone Saliba (Eds)

Washington, DC, The World Bank, 1996, xv + 62 pp., US$7.95, ISBN 0 8213 3653 3

The development of science and technology policy in developing countries has been relatively understudied—even more so the much needed policy reforms in these