

FOREWORD

Security and reliability are attributes that are very difficult to attain with any non-trivial assurance. Achieving both at the same time is even more difficult.

A frequent adage is that security or reliability is only as strong as its weakest link. However, what we have today is often merely a large assortment of poorly designed and badly implemented weak links: that is, weakness in depth rather than strength in depth. As a consequence, attackers and accidental causes have a major advantage over the defenders: exploits or malfunctions of only a few weak links (or, in some cases, only one) can result in chaos, whereas the defenders typically would need to ameliorate most of the serious weak links to prevent bad effects.

There is a long history of efforts devoted to the formulation of principles, adherence to which would tend to greatly increase the security, reliability, and trustworthiness of the resulting systems. Such principles go back at least as far as the Multics development that began in 1965, which led to my 1969 paper on “The Role of Motherhood in the Pop Art of System Programming,” and the fundamental 1975 paper by Jerry Saltzer and Mike Schroeder, “The Protection of Information in Computer Systems.”

This book is another significant step forward in that direction. Security and reliability are both emergent properties of an entire system, network of systems, or indeed an entire enterprise. Thus, it is absolutely essential that these critical attributes be considered in the large and that system developments seek to adhere to the best principles and to consciously strive to avoid bad experiences of past efforts. We must always remember that there are no easy answers when it comes to ensuring the trustworthiness of our systems and computer-based enterprises, especially in the presence of fallible or malicious people, flawed software, and faulty hardware. Eternal vigilance is the characteristic watchword, but following the good counsel found in this book can help significantly.

Peter G. Neumann

Principal Scientist in the Principled Systems Group of the Computer Science
Laboratory at SRI International

Author of *Computer-Related Risks* (Addison-Wesley), and Moderator of the ACM
Risks Forum

Menlo Park, California, USA, June 2005

