Foreword

Protecting valuable assets from intentional harm has been a focus of human activity from time immemorial. The proliferation of computers in society has meant that many business and mission critical assets are increasingly stored and manipulated by computer-based systems. The scale of misuse of these assets has also increased, because of their worldwide accessibility through the Internet and the automation of systems.

Security is concerned with the prevention of such misuse. While no system can be made completely secure, understanding the context in which a system will be deployed and used, the risks and threats of its misuse, and the systematic development of its software, are increasingly recognized as critical to its success. The cross-fertilization of systems development techniques from software engineering and security engineering offers opportunities to minimise duplication of research efforts in both areas, and, more importantly, to bridge gaps in our knowledge of how to develop secure software-intensive systems.

This book provides one of the first attempts to collect research work that draws upon software engineering to develop such systems more effectively. Contributions to this volume draw upon research and techniques from a range of software engineering activities, such as requirements engineering and specification, software patterns and design, and method and process-driven development.

An important secondary role of this book is to reach out and appeal to the traditional security engineering community to engage with — even guide — the software engineering community, in order to focus software engineering research on key issues of secure software systems development. If successful, these collected works may well provide the foundations for some seminal work in this area.

Bashar Nuseibeh
The Open University, UK
January 2006