Foreword

This excellent reference source offers a fascinating new insight into modern issues of security. It brings together contributions from an international group of active researchers who, between them, are addressing a number of the current key challenges in providing enterprise-wide information technology solutions.

The general area of security has long been acknowledged as vitally important in enterprise systems design; because of the key role it has in protecting the resources belonging to the organization and in ensuring that the organization meets its objectives. Historically, the emphasis has been on protecting complete systems and hardening the communications between trusted systems against external attack. Architects have concentrated on creating an encapsulation boundary supported by a trusted computing base able to control the access to all the available resources.

However, the themes selected for this book illustrate a change of emphasis that has been in progress over recent years. There has been a steady movement during this time towards finer grain control with the introduction of progressively more subtle distinctions of role and responsibility and more precise characterization of target resources. The controls applied have also become more dynamic, with increasing emphasis on delegation of responsibility and change of organizational structure, and the need for powerful trust models to support them. At the same time there has been a blurring of the traditional boundaries, because of the need for controlled cooperation and limited sharing of resources. The protection is in terms of smaller and more specialized resource units, operated in potentially more hostile environments.

Two examples may help to illustrate this trend. On the one hand, there is a need to protect information and privileges embodied in mobile devices. A mobile phone or PDA may contain information or access tokens of considerable sensitivity and importance, and the impact of loss or theft of the device needs to be bounded by system support that resists tampering and illicit use. On the other hand, digital rights management focuses on the protection against unauthorized use of items of information, ranging from software to entertainment media, which need to be subject to access controls even when resident within the systems managed by a potential attacker. Both these situations challenge the traditional complete system view of security provision.

These examples illustrate that the emphasis is on flexibility of the organizational infrastructure and on the introduction of new styles of information use. However, this is not primarily a book about mechanisms; it is about enterprise concerns and on the interplay that is required between enterprise goals and security solutions. Even a glance at the contents makes this clear. The emphasis is on architecture and the interplay of trust, threat and risk analysis. Illustrated by practical examples and concerns, the discussion covers the subtle relationship between the exploitation of new opportunities and the exposure to new threats. Strong countermeasures that rule out otherwise attractive organizational structures represent a lost opportunity, but business decisions that change the underlying assumptions in a way that invalidates the trust and risk analysis may threaten the viability of the organization in a fundamental way.

Nothing illustrates this better than the growing importance of social engineering, or phishing, styles of attack. The attacks are based on abuse of the social relationship that must be developed between an organization and its clients, and on the ignorance of most users of the way authentication works and of the dangerous side effects of communicating with untrusted systems. Countermeasures range from education and management actions to the development of authentication techniques suitable for application between mutually suspicious systems.

One of the messages to be taken from these essays is that security must be a major consideration at all stages in the planning and development of information technology solutions. Although this is a view that experts have been promoting for many years, it is still not universally adopted. Yet we know that retrofitting security to partially completed designs is much more expensive and is often ineffectual. Risk analysis needs to start during the formulation of a business process, and the enterprise needs a well-formulated trust model as an accepted part of its organizational structure. Only in this way can really well-informed technical choices be made about the information technology infrastructure needed to support any given business initiative. The stronger integration of business and infrastructure concerns also allows timely feedback on any social or organizational changes required by the adoption of particular technical solutions, thus reducing the risk of future social attacks.

For these reasons, the section on risk management and its integration with the software lifecycle is a fitting culmination of the themes presented here. It is the endpoint of a journey from technical architectures, through trust models and threat awareness to intelligent control of risks and security responses to them.

I hope this book will stimulate a greater awareness of the whole range of security issues facing the modern enterprise in its adoption of information technology, and that it will help to convince the framers of organizational policy of the importance of addressing these issues throughout the lifecycle of new business solutions, from their inception through deployment and into service. We all know that reduction of risk brings competitive advantage, and this book shows some of the ways in which suitable security approaches can do so.

Peter F. Linington
Professor of Computer Communication
University of Kent, UK

Peter Linington is a professor of computer communication and head of the Networks and Distributed Systems Research Group at the University of Kent. His current work focuses on distributed enterprise modeling, the checking of enterprise pattern application and policy-based management. He has been heavily involved in the development of the ISO standard architecture for open distributed processing, particularly the enterprise language. His recent work in this area has focused on the monitoring of contractual behaviour in e-business systems. He has worked on the use of multiviewpoint approaches for expressing distribution architectures, and collaborated regularly with colleagues on the formal basis of such system. He was been an advocate of model-driven approaches before they became fashionable, and experimented in the Permabase project with performance prediction from models. He is currently working on the application of model driven techniques to security problems. He has performed consultancy for BT on the software engineering aspects of distribution architectures. He has recently been awarded an IBM Faculty Award to expand work on the enhancement of the Eclipse modelling framework with support for OCL constraint checking.