Preface

Trust is firstly a social phenomenon. It is a multidimensional, multidisciplinary, and multifaceted concept. Various definitions exist in the literature. Common notions are confidence, belief, and expectation regarding the reliability, integrity, ability, or characters of an entity. In general, trust is subjective because acceptably sufficient trust levels differ for each entity. It is also dynamic, affected by many factors. It can further develop and evolve due to good experience. Bad experience, however, can cause decay due to sensitivity. From the digital system point of view, trust is an assessment on a trusting object based on the criteria of a trusting subject and a number of trust attributes (e.g., competence, security, dependability, and so on).

Trust plays a crucial role in our social life. With the rapid development of mobile communication and networking technologies, trust has become an important factor that influences the success of our digital life in mobile environments. Trust modeling and management are a useful means to control and manage trust in mobile computing systems. Transforming from a social concept of trust to a digital concept, trust modeling and management help in designing and implementing a trustworthy digital system, especially in emerging mobile computing systems and environments (e.g., self-organized mobile computing systems such as ad hoc networks and pervasive systems, etc.). Nowadays, trust management is emerging as a promising technology to facilitate collaboration among entities in a mobile environment where traditional security paradigms cannot be enforced due to lack of centralized control and incomplete knowledge of the environment.

The method to specify, evaluate, set up, and ensure trust relationships among entities is the trust model. The trust model aids the digital processing and/or controlling of trust. Trust management is concerned with: collecting the information required to make a trust relationship decision, evaluating the criteria related to the trust relationship as well as monitoring and reevaluating existing trust relationships, and automating the above process. However, an extension of this definition is needed to automatically ensure a dynamically changed trust relationship towards autonomic trust management. More importantly, due to the subjective characteristic of trust, trust management should also consider the role and influence of human beings. It is preferred that the design of trust management system is human-centric.

This book aims to provide a single record of current technologies and applications in Trust Management (TM), especially focusing on autonomic and usable TM in mobile environments. The overall objectives are to investigate various definitions or understandings of trust and extract its characteristics; study how to model trust in a digital approach and implement the model for establishing and managing trust in a mobile system; overview the literature of TM in mobile computing; summarize the achievement of TM in mobile cloud computing, mobile social networking, and future mobile Internet; and introduce autonomic and usable trust management solutions in the mobile domain. Regarding future research trends, the book indicates special issues needed to be solved for practical deployment of trust management systems in mobile computing environments.
Research on trust modeling and management is a prosperous area. It has become important in recent years because this technology can be applied to various areas to construct a trustworthy, secure, and dependable system, especially when collaboration of system entities is needed. Current research ultimately aims to empower individuals and organizations in building competencies for exploiting the opportunities of trustworthy mobile environments.

This book is designed for a professional audience who wishes to learn about the state of the art in trust modeling and management. More specifically, the book offers theoretical perspective and practical solutions to graduate and post-graduate students, researchers, and practitioners working in the areas of trust, security, and privacy in mobile computing systems (e.g., ad hoc networks, pervasive and ubiquitous computing, mobile computing platforms, social networking, grid computing, cloud computing, and software systems, etc.). This book is also suitable as a supplemental text or reference book for the graduate level or post-graduate level, as well as advanced undergraduate students in computer science, information science, computer engineering, Information Technology (IT), and electrical engineering.

This book integrates autonomic and usable trust management together and provides the latest research, development, and application results in this field to researchers, engineers, advanced undergraduates, and graduate students who are interested in the technologies and applications of TM. The proposed book will:

- Concern both subjective and dynamic characteristic of trust;
- Focus on autonomic and usable trust modeling and management technologies and solutions;
- Identify new requirements and challenges of TM in different scenarios of mobile environments;
- Present the latest research and development results in the focused topics;
- Investigate how some advanced technologies can be applied into mobile computing systems; and
- Be involved in more complete issues related to TM in mobile environments (e.g., privacy enhancement and key management, for practical system deployment).

Special attention will be paid to autonomic and usable trust modeling and management. More importantly, we aim to reveal how to achieve user trust and human-computer trust interaction and how to apply a human-centric trust modeling and management methodology into developing practical solutions.

The nine chapters of this book:

- Investigate various definitions or understandings of trust and its characteristics;
- Overview the literature of trust modeling and management in mobile networking, computing, and communications, analyzing current research issues and discussing future research trends;
- Study the recent advances of trust management in mobile environments and explore usable and autonomic trust management solutions for mobile cloud computing, unwanted traffic control, trustworthy pervasive social networking, and human-computer trust interaction; and
- Provide practical and comprehensive solutions for usable and autonomic trust management based on both trusted computing technology and trust evaluation by applying an inter-disciplinary methodology.
The prospective audience would be anyone who is interested in trust, security, and privacy: academics, technical managers, socialists, psychologists, and information security officers. The book can be used as a reference to achieve a general overview of trust modeling and management. It could serve as a textbook or reference materials for undergraduate and/or postgraduate teaching. IT industrial designers and architects may also refer to this book when designing and developing a practical trust management system in mobile environments.

**ORGANIZATION OF THE BOOK**

This book is organized into three sections, with a total of nine chapters. The first section introduces the technical background of trust modeling and management, which includes three chapters. This section also acts as tutorial material for a wide range of audiences, including advanced undergraduate students of IT.

**Section 1: Background – Trust, Trust Modeling, and Trust Management**

**Chapter 1: Perspective and Characteristics of Trust – Understanding Trust in Different Disciplines**

Chapter 1 introduces various perspectives of trust in different disciplines, investigates the factors that influence trust, and summarizes its basic characteristics. As the first chapter, it also introduces the contents and structure of the whole book, as well as the internal-relationships of the nine chapters.

**Chapter 2: Trust Modeling and Computational Trust – Digitalizing Trust**

Chapter 2 introduces the theories of trust modeling and computational trust. It classifies existing trust models based on different criteria, introduces a number of technologies applied in trust evaluation, and discusses the current problems and challenges in the literature.

**Chapter 3: Trust Management and Its Challenges**

Chapter 3 briefly introduces trust management technologies and gives a couple of concrete example solutions for the purpose of tutorial illustration. In addition, it discusses the current issues, problems, other interesting application scenarios, and future research trends in the area of trust management.

The second section introduces the current advances of trust management in mobile environments, focusing on mobile cloud computing, pervasive social networking, and the future Internet. It includes three chapters.
Section 2: Current Advances of Trust Management in Mobile Environments

Chapter 4: Trust Management in Mobile Cloud Computing

Chapter 4 introduces the advances of trust management technologies in cloud computing and mobile cloud computing. It analyzes the basic requirements of trust management in mobile cloud computing based on its architecture and distinct characteristics. This chapter further proposes a number of schemes in order to automatically control data access based on trust evaluation in a mobile cloud computing environment. Unsolved issues and future research challenges are also discussed.

Chapter 5: Trust Management for Unwanted Traffic Control

Chapter 5 discusses applying a trust management technology to conduct unwanted traffic control on the Internet, especially the mobile Internet. This chapter proposes a generic unwanted traffic control solution through trust management. It can control unwanted traffic from its source to destinations in a personalized manner according to trust evaluation at a Global Trust Operator and traffic and behavior analysis at hosts. Thus, it can support unwanted traffic control in both a distributed and centralized manner and in both a defensive and offensive way.

Chapter 6: Trust Management in Pervasive Social Networking

Chapter 6 reviews the literature with regard to how to build up trust in pervasive social networking. It explores whether pervasive social networking is demanded, considering many existing popular Internet social networking services. It proposes a trust management framework that holistically supports context-aware trust/reputation generation, trustworthy content recommendations, secure communications, unwanted traffic control, user privacy recommendation, and secure face-to-face pervasive social communications.

Although the chapters in Section 2 touch either autonomic or usable trust management solutions here and there in several concrete mobile domains, both autonomic and usable TM are not discussed in an oriented or specific manner. The third section further introduces a number of solutions for both autonomic and usable trust management in mobile environments. The contents of Section 3 further show the particular advance of trust management in mobile environments towards practical deployment, system intelligence, and social acceptance.

Section 3: Autonomic and Usable Trust Management in Mobile Environments

Chapter 7: User Trust and Human-Computer Trust Interaction

Chapter 7 explores the factors that influence trust in human-computer interaction (i.e., the construct of Human-Computer Trust Interaction [HCTI]) and proposes a number of instructions to improve user trust for human-computer interaction. This chapter discusses the ways for improving usability of trust management.
Chapter 8: Autonomic Trust Management in Mobile Environments

Chapter 8 introduces an autonomic trust management solution in mobile environments by applying both trusted computing and trust evaluation technologies. Its applicability is illustrated by applying it to a number of mobile application scenarios.

Chapter 9: Usable Trust Modeling and Management

Chapter 9 introduces a human-centric trust modeling and management method in order to design and develop a usable trust management solution that can be easily accepted by users towards practical deployment. Its effectiveness is illustrated by applying it to the design of a reputation system for mobile applications in order to achieve both usable and autonomic trust management.

Towards autonomic and usable trust modeling and management, the book covers the entire scope of studies for developing a trustworthy mobile system: from mobile Internet unwanted traffic control to mobile social networking, from mobile cloud computing to various mobile systems, from system framework and architecture to user interface and human-computer interaction. The book provides a comprehensive study on usable and autonomic trust management system development. Writing this book has been an enlightening and thought-provoking experience for me. I hope you enjoying reading this book. I will be happy if you find this book helpful and your interest in the field of trust modeling and management further aroused by reading the various perspectives presented herein.

Zheng Yan
Xidian University, China & Aalto University, Finland