

# Chapter 18

## Trust Modeling and Management: From Social Trust to Digital Trust

**Zheng Yan**

*Nokia Research Center, Finland*

**Silke Holtmanns**

*Nokia Research Center, Finland*

### ABSTRACT

*This chapter introduces trust modeling and trust management as a means of managing trust in digital 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 distributed systems. Furthermore, the authors hope that understanding the current challenges, solutions and their limitations of trust modeling and management will not only inform researchers of a better design for establishing a trustworthy system, but also assist in the understanding of the intricate concept of trust in a digital environment.*

### INTRODUCTION

Trust plays a crucial role in our social life. Our social life is characterized by the trust relationships that we have. Trust between people can be seen as a key component to facilitate coordination and cooperation for mutual benefit. Social trust is the product of past experiences and perceived trustworthiness. We constantly modify and upgrade our trust in other people based on our

feelings in response to changing circumstances. Often, trust is created and supported by a legal framework, especially in business environments or when financial issues are involved. The framework ensures that misbehavior can be punished with legal actions and increases the incentive to initiate a trust relationship. The legal framework decreases the risk of misbehavior and secures the financial transactions. With the rapid growth of global digital computing and networking

DOI: 10.4018/978-1-4666-2803-8.ch018

technologies, trust becomes an important aspect in the design and analysis of secure distributed systems and electronic commerce. However, the existing legal frameworks are often focused on local legislation and are hard to enforce on a global level. The most popular examples are email spam, software piracy, and a breach of warranty. Particularly, because legal regulation and control cannot keep pace with the development of electronic commerce, the extant laws in conventional commerce might not be strictly enforceable in electronic commerce. In addition, resorting to legal enforcement in electronic commerce might be impracticably expensive or even impossible, such as in the case of micro payment transactions (Ba, Whinston, & Zhang 1999). This raises the importance of trust between interacting digital entities. People cannot assume that the legal framework is able to provide the needed trustworthiness for their digital relationships, for example, for an electronic transaction purpose. It has been a critical part of the process by which trust relationships are required to develop in a digital system. In particular, for some emerging technologies, such as MANET (Mobile Ad Hoc Networks), P2P (Peer-to-Peer) computing, and GRID virtual systems, trust management has been proposed as a useful solution to break through new challenges of security and privacy caused by the special characteristics of these systems, such as dynamic topology and mobility (Lin, Joy, & Thompson, 2004; Yan, 2006; Yan, Zhang, & Virtanen 2003).

Trust is a very complicated phenomena attached to multiple disciplines and influenced by many measurable and non-measurable factors. It is defined in various ways for different purposes and cultures, even though in information technology area. Thereby, it is difficult to have a common definition for this comprehensive concept.

Establishing a trust relationship in digital networking environment involves more aspects than in the social world. This is because communica-

tions in the computing network rely on not only relevant human beings and their relationships, but also digital components. On the other hand, the visual trust impression is missing and need somehow to be compensated. Moreover, it is more difficult to accumulate accurate information for trust purposes in remote digital communications where information can be easily distorted or faked identities can be created. The mapping of our social understanding of trust into the digital world and the creation of trust models that are feasible in practice are challenging. Trust is a special issue beyond and will enhance a system security and personal privacy. Understanding the trust relationship between two digital entities could help selecting and applying feasible measures to overcome potential security and privacy risk. From social trust to digital trust, how can trust theory help in designing and implementing a trustworthy digital system? The literature suggests the usage of trust modeling and management. This book chapter aims to help readers understanding trust modeling and management in the emerging technologies. The reader is guided from the creation of a digital trust concept to the deployment of trust models for trust management in a digital environment.

## **BACKGROUND**

The problem to create trust in the digital environment has led to a number of approaches, for example, expressing and modeling trust in a digital way, evaluating trust in a reputation system, rating agencies, certificate authorities that equip trading partners with certificates as trusted providers and brokers, trustworthy user interface design, and so on. Current academic and industrial work related to trust covers a wide area of interest ranging from such aspects as perception of trust, cryptographic-security enforced trust solutions, trust modeling, and trust management to trusted computing activities.

23 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/trust-modeling-management/74120](http://www.igi-global.com/chapter/trust-modeling-management/74120)

## Related Content

---

### Computational Trust in SocialWeb: Concepts, Elements, and Implications

Kiyana Zolfagharand Abdollah Aghaie (2010). *International Journal of Virtual Communities and Social Networking* (pp. 60-74).

[www.irma-international.org/article/computational-trust-socialweb/45779](http://www.irma-international.org/article/computational-trust-socialweb/45779)

### Social Capital, Self-Esteem, Popularity, Need for Accessibility to Friends, and Stress Predict Cyber Technology Use

Champika K. Soysaand Jennifer M. Gardner (2019). *Internet and Technology Addiction: Breakthroughs in Research and Practice* (pp. 595-612).

[www.irma-international.org/chapter/social-capital-self-esteem-popularity-need-for-accessibility-to-friends-and-stress-predict-cyber-technology-use/228881](http://www.irma-international.org/chapter/social-capital-self-esteem-popularity-need-for-accessibility-to-friends-and-stress-predict-cyber-technology-use/228881)

### Designing for Trust

Piotr Cofta (2009). *Handbook of Research on Socio-Technical Design and Social Networking Systems* (pp. 388-401).

[www.irma-international.org/chapter/designing-trust/21421](http://www.irma-international.org/chapter/designing-trust/21421)

### Effects of Computer Self Efficacy on the Use and Adoption of Online Social Networking

Lionel Mewand William H. Money (2010). *International Journal of Virtual Communities and Social Networking* (pp. 18-34).

[www.irma-international.org/article/effects-computer-self-efficacy-use/43064](http://www.irma-international.org/article/effects-computer-self-efficacy-use/43064)

### The Politics of e-Learning: A Play in Four Acts

Celia Romm Livermore, Mahesh Raisinghaniand Pierluigi Rippa (2015). *International Journal of E-Politics* (pp. 30-42).

[www.irma-international.org/article/the-politics-of-e-learning/127688](http://www.irma-international.org/article/the-politics-of-e-learning/127688)