IRM PRESS
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.irm-press.com

ITB15312

This chapter appears in the book, ***Computer Security, Privacy, and Politics: Current Issues, Challenges, and Solutions*** by **R. Subramanian** © 2008, IGI Global

Chapter XIII

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.

Copyright © 2008, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

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 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 can not 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 communications 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

Copyright © 2008, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

32 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/6870

Related Content

Two-Stage Automobile Insurance Fraud Detection by Using Optimized Fuzzy C-Means Clustering and Supervised Learning
Sharmila Subudhiand Suvasini Panigrahi (2020). *International Journal of Information Security and Privacy (pp. 18-37).*
www.irma-international.org/article/two-stage-automobile-insurance-fraud-detection-by-using-optimized-fuzzy-c-means-clustering-and-supervised-learning/256566

Do Privacy Statements Really Work? The Effect of Privacy Statements and Fair Information Practices on Trust and Perceived Risk in E-Commerce
Hamid R. Nematiand Thomas Van Dyke (2009). *International Journal of Information Security and Privacy (pp. 45-64).*
www.irma-international.org/article/privacy-statements-really-work-effect/4001

Enhancing Security at Email End Point: A Feasible Task for Fingerprint Identification System
Babak Sokoutiand Massoud Sokouti (2013). *Theory and Practice of Cryptography Solutions for Secure Information Systems (pp. 361-404).*
www.irma-international.org/chapter/enhancing-security-email-end-point/76523

A TPM-based Secure Multi-Cloud Storage Architecture grounded on Erasure Codes
Emmy Mugisha, Gongxuan Zhang, Maouadj Zine El Abidineand Mutangana Eugene (2017). *International Journal of Information Security and Privacy (pp. 52-64).*
www.irma-international.org/article/a-tpm-based-secure-multi-cloud-storage-architecture-grounded-on-erasure-codes/171190

Current Network Security Systems
Göran Pulkkis, Kaj Grahnand Peik Astrom (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications (pp. 1339-1348).*
www.irma-international.org/chapter/current-network-security-systems/23161