Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 85 (2016) 527 – 534

Procedia Computer Science

International Conference on Computational Modeling and Security (CMS 2016)

A Survey of Trust Models for Enterprise Information Systems

Asmita Manna[a,*], Anirban Sengupta[a], Chandan Mazumdar[a]

[a]*Centre for Distributed Computing, Dept. of Computer Science and Engineering, Jadavpur University, Kolkata-700032,India*

Abstract

Most of today's enterprises are open in a competitive market worldwide and dependent on distributed information infrastructure across various geospatial location and various cyber spatial location as well with a purpose of offering ready and effective services to customers. But this decentralization comes at the cost of security. The distributed computing framework is vulnerable to attacks from malicious agents, thereby increasing the chances of risks and security breaches. Trust and Reputation management system is a tool to combat security threats. A trust management system helps its user to decide how trustworthy the other party is before making a transaction. This work aims to identify the required characteristics of trust needed for an enterprise network and presents a survey of a few well known trust models with an aim to identify trust characteristics in each model.

Peer-review under responsibility of the Organizing Committee of CMS 2016

Keywords: Trust Model, Enterprise Information System

1. Introduction

From social science perspective, trust is an essential parameter for any type of transaction among human beings. Additionally, trust is also needed for all automated information processing systems. In computer science research, formal studies on trust and reputation have been undertaken in various areas like security and access control, reliability and robustness of distributed systems, and policies for decision making under uncertainties, particularly in the area of e-commerce. However, in the domain of Enterprise Information System (EIS), trust is a relatively new paradigm. In case of enterprise information systems, notion of trust has only been considered in credential checking for access controls. But, in today's scenario, when enterprises are open in a competitive market worldwide with a major share in open systems like internet and cloud, they are more vulnerable to attacks. To make enterprises more secured and attack-resilient, trust values of different stakeholders should be considered before allowing any kind of

Peer-review under responsibility of the Organizing Committee of CMS 2016
doi:10.1016/j.procs.2016.05.212

transaction or information communication. Most of the existing credential-based trust models do not consider the past behavior or reputation of a stakeholder; experience-based trust models do not differentiate among different contexts of trust evaluation; most social science models cannot evaluate trust in a measurable form; distributed system trust models only focus on aspects of secure communication. It can be seen that there is not a single available trust model which can cater to the different requirements of EIS, while being compatible with existing security policies of the enterprise. In this paper, a survey of available trust models based on required and identified attributes is presented. The paper looks at the pros and cons of the models with an aim to enable researchers to develop a comprehensive trust model for EIS that will be able to generate useful and usable security policies. The rest of the paper is organized as follows. Section 2 defines the need of trust evaluation from EIS perspective; Section 3 defines the taxonomy of trust and reputation; Section 4 discusses about required attributes of trust model; Section 5 presents a brief description of models and a table showing the comparison of different trust models; finally, Section 6 concludes the paper.

2. Need of trust evaluation for enterprise

According to current enterprise information system scenarios, users can be divided into three categories: organizational personnel, customers and visitors. Among them, organizational personnel directly interact with the IT and non-IT resources of an enterprise; hence, they have the maximum opportunity of misusing the systems. Personnel, with only a minimum level of trust value, should be allowed access to the EIS. But those values must not be static; instead they should evolve with time, based on their interaction with the system. To assign the trust value for first time, EIS has to heavily rely on credentials and background checking.

Customers are the most important users and the basic goal of the enterprise should be to satisfy customers. They are exposed to only a small portion of EIS resulting in very little chance of harming the system physically. However, dissatisfied customers can harm the intangible assets of an enterprise. Particularly in today's virtual world, a customer's feedback and thoughts can easily be propagated to others in no time. So, to protect its reputation and goodwill, an enterprise cannot afford to allow erroneous feedback; there lies the usage of trust evaluation for customers.

Visitors are neither exposed to resources, nor do their feedback carry much value for an enterprise. That is why not many precautions are taken regarding visitors, leaving them with a probability of harming the enterprise in an unexpected way. So there must be a trust value evaluation for each visitor before permitting him/her in the enterprise's physical premises or virtual premises as well. Credential-based trust evaluation is the basic manner of trust value evaluation of a visitor.

3. Taxonomy of trust models

There has been a lot of research related to trust evaluation in computer science. They can be classified into three major categories:

a. Credential-based trust: Credentials are testimonials or certified documents showing the qualification or status of an individual that entitles him to certain services and powers. Here it is assumed that trust is established by verifying certain credentials and once trust is established, access rights to different resources are granted using pre-defined policies. These are widely used in access control.

b. Reputation-based trust: Reputation is nothing but the cumulative knowledge about past behavior of an entity and relevant events and interactions of the entity with an agent. Based upon that knowledge, it is predicted how that entity will behave in future. This knowledgebase can be created in two ways: direct experience of truster or, if direct interaction is not available, recommendation from other agents can be taken into account. The complexity associated with recommendations is high because it introduces uncertainty, as recommenders can manipulate or conceal parts of true information for their own benefit, leading to the breakdown of the Trust and Reputation model. These models even compute trust over a social relationship or across a third-party recommender based path. Reputation, either via direct trust or recommended trust, forms the core of trust modeling in general.

c. Trust in information resource:

In both credential-based and recommendation-based system, the basis of trust formation starts with a known attribute; either credential which is ideally provided by a trusted organization or by past behaviors, either judged by truster itself or based on others' interactions. However, in web-based information systems, these third parties