Knowledge-Based Systems 106 (2016) 150–163

Contents lists available at ScienceDirect

Knowledge-Based Systems

journal homepage: www.elsevier.com/locate/knosys

A survey of trust management systems for online social communities – Trust modeling, trust inference and attacks

Yefeng Ruan*, Arjan Durresi

Indiana University Purdue University Indianapolis, Department of Computer and Information Science, Indianapolis, IN 46202 USA

ARTICLE INFO

Article history:
Received 14 September 2015
Revised 19 May 2016
Accepted 21 May 2016
Available online 25 May 2016

Keywords:
Online trust
Trust management
Online social communities
Attack

ABSTRACT

Trust can help participants in online social communities to make decisions; however, it is a challenge for systems to map trust into computational models because of its subjective properties. Also, many online social communities are sparsely connected. Therefore, it is necessary to introduce mechanisms which can infer indirect trust among participants who are not directly connected. We provide a survey of existing trust management systems for online social communities. We also list four types of attacks, and analyze existing systems' vulnerabilities. Compared with previous surveys, our survey takes trust modeling, trust inference, and attacks into account. Although there are several survey papers about global trust/reputation related attacks, the main contribution of this paper is that we consider trust inference and potential local trust related attacks.

1. Introduction

Due to the development of the Internet and computer-based devices, especially smart phones, people are now moving at least part of their social activities to online environments. In the last few years, many online social networks, such as Facebook and Twitter, have spread out around the world. Participants in such kinds of social networks can have a large number of claimed friends. Some of them may be well known, while some are not. One possible way to deal with this problem is to differentiate them by using trust metrics. Huberman et al. [1] differentiate "claimed friends" from "real friends" in Twitter by counting the number of interactive tweets that two users post toward each other. Besides social networks, many other online applications also exhibit social properties, for example e-commerce [2–4], like eBay [5], Amazon and Epinions [6,7], and P2P file sharing networks [8,9]. In this paper, we call them online social communities in which participants can be users, agents, devices, or others.

We have seen that trust plays an extremely important role in online social communities, as well as in people's lives; however, there are some challenges in applying trust in online social communities [10]. First of all, we have to represent trust in a computational model. Trust is not easy to model in a computational way because of its subjective property [11]. Also, it cannot be applied directly in online social communities due to different features that online social communities have from traditional social networks [12]. For example in real life, people only have a limited number of friends to evaluate, but this number explodes in online social communities. On Facebook and Twitter, users can have thousands of friends. Apart from this, in real life, trust is developed slowly over time, based on face-to-face social experiences; however, this is very difficult in online social communities due to the large number of potential friends. Therefore, trust in online social communities must be computational such that it can be processed by computers [11,12]. The difficulty is that trust is a subjective concept, and it has different meanings in different fields and applications [13,14]. For example, in Amazon, participants use stars to represent to what extent they think others' reviews are useful. While in other cases, such as in P2P networks, trust measures the quality of downloaded files, downloading speed, and so on [8,15]. Therefore, trust modeling should be dependent on applications or scenarios. In the remainder of this paper, we use the term trust modeling to denote how to represent trust in a computational way.

Besides trust modeling, another challenge is how to infer indirect trust information among two unconnected participants. In many online communities, only a small number of participants are directly connected, compared with the potential number of pairs of participants. Many works have shown that online communities are sparsely connected [1,7,12,16,17]. Therefore, it is urgent to introduce mechanisms that can be used to infer indirect trust among participants who are not directly connected. Such type of framework is described as "Friend of a Friend (FOAF)" in [18]. Basically,

* Corresponding author.
E-mail addresses: yefruan@cs.iupui.edu (Y. Ruan), durresi@cs.iupui.edu (A. Durresi).

http://dx.doi.org/10.1016/j.knosys.2016.05.042
0950-7051/

trust propagates along chains; however, how to propagate trust is still an open debate. Both general and application specific mechanisms are proposed by many researchers in this field [19–28].

In this paper, we use the term trust management systems to denote the systems dealing with how to represent, infer, and use trust. We provide a survey for existing trust management systems used in various online social communities. We mainly focus on two challenges – trust modeling and trust inference. Although there are several survey papers about computational trust [29–31] and global trust/reputation related attacks [32–34], the main contribution of this paper includes:

- We provide a survey for trust inference problem, which takes into account inferring indirect trust relationship for not directly connected participants.
- We provide a survey for four types of local trust related attacks, and analyze existing schemes' vulnerabilities to them.

The rest of this paper is organized as follows: in Section 2, we investigate various definitions of trust, and introduce some related works. In Section 3, we review how existing works deal with the first challenge – trust modeling. In Section 4, we illustrate the second challenge – trust inference, and survey several existing schemes. In Section 5, we illustrate four types of attacks in trust management systems. In Section 6, we analyze existing schemes' vulnerabilities to four types of attacks. In Section 7, we conclude the paper.

2. Background and related works

2.1. Definition of trust

Trust is a relationship existing between two participants. In this paper, we use truster and trustee to denote them. Trustee is the participant being evaluated by the truster. For example, when we say *A* trusts *B, A* is the truster and *B* is the trustee.

Trust is studied and used in a number of disciplines, such as sociology, psychology, economics, computer science, and so on. As a result, there are many definitions for trust and no general consensus has been achieved so far [35,36]. Among them, one of the recent summarized definition is given by [36]:

> "Trust is the willingness of the trustor (evaluator) to take risk based on a subjective belief that a trustee (evaluatee) will exhibit reliable behavior to maximize the trustor's interest under uncertainty (e.g., ambiguity due to conflicting evidence and/or ignorance caused by complete lack of evidence) of a given situation based on the cognitive assessment of past experience with the trustee" [36].

In this definition, trust is explained as the probability of performing a specific action. In the field of computer science, besides probability, there are many other representations of trust, such as entropy [37,38], similarity [39–41], and so on. We will see different types of representations of trust in the following.

Trust can be classified based on various criteria. In [42], McKnight classified it into three categories: impersonal/structural trust, dispositional trust, and personal/interpersonal trust. Impersonal/structural trust is determined by institutional properties rather than by participants themselves. Dispositional trust represents participants' bias trust preferences. Personal/interpersonal is the participant-to-participant trust relationship. Among them, personal/interpersonal trust has attracted ample attention from researchers. In this paper, we mainly focus on personal/interpersonal trust. For simplicity, we call it trust in the following. Trust can be further divided into functional trust and recommender trust based on the types of behaviors [43]. Functional trust describes how trustworthy a person is when implementing functions, e.g. how good Alice is as a doctor. Recommender trust measures how reliable a person's recommendations are, e.g. how reliable Alice's recommendations are about doctors.

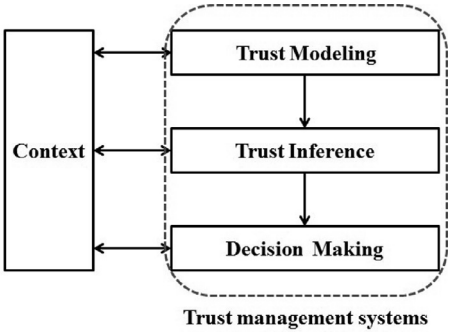

Fig. 1. Framework of trust management systems.

Trust has many properties, such as subjective, dynamic, asymmetric, context dependent, transitive, composable, and so on [11,13,29]. Similar to its definition, different applications highlight different aspects of its properties.

2.2. Trust management systems

Trust management systems are designed to help participants to make better decisions based on trust information. According to Ries et al. [31], trust management systems can be divided into three parts: trust modeling, trust management and decision making. Trust modeling mainly deals with how to represent trust relationships in computational models, and trust management is used to describe how to collect evidence and to do risk evaluation. Decision making is another important and complicated field, and can even be treated separately [31]. As trust modeling and trust management, together, mainly deal with how to represent trust in computational models using available raw data, we incorporate them together and use trust modeling to represent them. Apart from them, we also include trust inference into trust management systems as it is a very important component for trust management systems to work more intelligently and efficiently. Trust inference uses direct trust information among participants to infer indirect trust information. In this paper, we mainly focus on trust modeling and trust inference.

We represent the framework of trust management systems in Fig. 1. All three phases are dependent on context or applications, especially trust modeling and decision making. For example, depending on the type of available data, systems would map appropriately the raw data into defined trust metrics. Similarly, depending on context, such as risk, systems might use different methods to aggregate and filter trust, in trust inference. Finally, in decision making, for example, systems might apply different levels of trust thresholds when participants select a doctor for an important surgery, compared with when they decide whether or not to watch a movie. Furthermore, the three above phases are interrelated. So, the accuracy of trust inference, and its corresponding level of support in decision making will depend on the availability and granularity of raw trust data from the field.

2.3. Related works

As online social communities are becoming more popular, there are also more works investigating trust relationships in this field of computer science. As a result, there are several survey papers in this field.