Computers and Electrical Engineering 000 (2016) 1–15

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

A risk evaluation approach for authorization decisions in social pervasive applications☆

Amr Ali-Eldin[a,*], Jan van den Berg[b,c,d], Hesham A. Ali[a]

[a] Computer Engineering and Control Systems Department, Faculty of Engineering, Mansoura University, Mansoura, Egypt
[b] Cyber Security Academy The Hague (CSA), Leiden University, The Netherlands
[c] Faculty of Technology, Policy and Management, Delft University of Technology, Delft, The Netherlands
[d] Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, Delft, The Netherlands

ARTICLE INFO

Article history:
Received 14 June 2015
Revised 21 January 2016
Accepted 22 January 2016
Available online xxx

Keywords:
Security risks
Authorization
Social networks
Social Network Services (SNS)
Social pervasive applications
Neuro-fuzzy systems

ABSTRACT

Most research in social networks has focused on the assumption that unknown entities are malicious and thus the traditional approach was to detect them and deny their access to sensitive data. In this paper, we propose a new computational model that helps users predict security risks associated with their information sharing on social networks. The model is based on the assumption that a risk indicator value can be predicted by assessing a number of risk attributes using a neuro-fuzzy technique. A disclosure decision is made based on this risk indicator value. The approach was tested in a real prototype of a social mobile service at a university campus. Further, we show how the model can be implemented in a popular social rating site. Results obtained show the relevance and effectiveness of the proposed approach in predicting risks and in deciding up on it about disclosure decisions in social pervasive applications.

1. Introduction

The recent technological IT-developments in pervasive telecommunication networks and devices have paved the way for what is known as pervasive computing leading to the deployment of ubiquitous services [1–3]. Further, the introduction of the latest technology of smart phones with GPS capabilities led to a complete set of location-based services (LBS) in addition to social network sites (SNSs) and associated pervasive applications.

There is no doubt that privacy and security can represent challenges for the adoption of social pervasive applications [4]. Most scientific literature in this domain assumed the non-trustworthiness of unknown entities by default and thus the conventional approach was to block all requests coming from unknown entities to sensitive information using technological approaches such as cryptographic solutions and access control mechanisms [5,6]. Social pervasive applications are considered highly dynamic and data rich environments with lots of possibilities for the exposure of users' sensitive data. In this context, users' authorizations decisions are of dynamic nature and should take into consideration the limited computing resources of pervasive devices and limited bandwidth of pervasive networks.

Most research, in social networks, has focused on interactions among users while a few researches have considered third party application interactions [7]. In this paper, we propose an autonomous approach to risk management that takes into

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. H. Vahdat-Nejad.

* Corresponding author.
E-mail address: dr.amr.ali-eldin@ieee.org (A. Ali-Eldin).

http://dx.doi.org/10.1016/j.compeleceng.2016.01.022
0045-7906/

consideration user interactions as well as other entities' interactions based on a risk indicator model. The paper is organized as follows: in the next section, we elaborate on related work. Then, we introduce the proposed model. Then, we present a case study followed by a discussion of the obtained results and performance evaluation. Finally, we conclude the paper highlighting potential future work.

2. Related work

The possibility of retrieving and mining sensitive information from social network sites (SNS) has raised many concerns on user privacy. Nowadays, most web applications use application programming interfaces (APIs) and integration mechanisms such as the representational state transfer (REST) protocol, simple object access protocol (SOAP) and web services to retrieve users' profiles from SNS [7]. Privacy threats are caused by the linkage between personally identifiable information (PII) and sensitive data [8]. Therefore, most scientific literature in this domain has focused on the separation between both types of information using approaches such as anonymity solutions, access control mechanisms and data encryption [9,10].

Controlling the access to sensitive information in social networks though challenging may represent a realistic approach [7]. This can be achieved by controlling access to sensitive data or by enforcing user authorization decisions and access control mechanisms. Authorization decision making requires that data collection policies of information requestors (IR's) be communicated beforehand. Besides, users should be able to describe their privacy requirements. Moreover, trust plays an important role since users can be divided into trusted (friends) and non-trusted (unknown) ones. A number of research efforts has followed this approach such as [11–13]. In [11], a sophisticated rule-based access control was proposed which used certificates and authorization tokens to identify trusted users. In [12], a policy based application was presented for information sharing using other users recommendations. Despite these might seem sophisticated approaches, they lack the support to adapting to changes in user privacy and trust requirements as well as having the users heavily involved in controlling access to their data.

In the social network domain; a new approach is needed that adapts its functionalities to changes while minimizing users interactions. In [14], ShEM was proposed to enable users to dynamically (both manually and automatically) control their information disclosure decisions through the use of a Mamdani fuzzy inference system. Nevertheless, the ShEM approach like many others depends on a shared repository which has to be trusted and may represent a single point of failure. Avoiding the use of a shared repository may present another requirement for a private and trusted social network platform. Having said that, mechanisms are needed so that users can have dynamic control of their personal information disclosure. In this context, some efforts have focused on the use of peer-to-peer (P2P) or decentralized network topologies in the provisioning of social applications. Among these efforts is PeerSon which is a P2P system that facilitates social network activities among users relying on encryption mechanisms [15]. Another approach, the Safebook [16] is a decentralized architecture for information exchange between users where trust relationships are taken into consideration in the authorization decisions. Although these systems can help protect users' privacy, because they avoid the use of a centralized repository, they add complexities because users have to self-manage their personal data storage and usage. Moreover, they may suffer from system performance issues due to the overhead associated with encrypting and decrypting taking place for every communication.

The proposed approach represents a new approach since it takes the above-mentioned issues into consideration; adapting to changes, minimizing users interactions and users access control to data. User data is controlled by the users themselves while avoiding the use of decentralized systems and associated complexities. This is achieved through the use of a services approach deployed partially on the user device and partially on an Internet application server via the Cloud. This service communicates with the user device through the Internet using an android mobile application running from the user mobile device. This way we are able to offload heavy computations to the server side minimizing network traffic by sending only needed information over the network. In addition, information is sent only after risks have been defined using a risk evaluation and an authorization decision models which will be discussed in the next section.

3. The proposed model

Uncertainty associated with information disclosure in pervasive networks makes it difficult to make a good decision on information disclosure [17,18]. In the social context, users are surrounded by many uncertainties; unknown third-party applications and other unknown users who would like to get access to sensitive information. Further, security risks do exist which are caused by these uncertainty conditions. Sharing information under uncertainty conditions while being able to guarantee security represents one of the challenges in these environments [14]. The authors' research hypothesis is that risk prediction and weighing is critical in social environments and can lead to successful protection of user data. This hypothesis is tested in the paper by the use of a case study. Based on this research hypothesis, the risk-based authorization model is proposed (see Fig. 1). In the following, the components of this model are being introduced.

3.1. Risk indicator (KI)

The authors assume that it is more convenient for users to specify a security risk rather than to make an authorization decision. The reason for that is that one can think a certain interaction to put one's privacy in risk but still be willing to

Please cite this article as: A. Ali-Eldin et al., A risk evaluation approach for authorization decisions in social pervasive applications, Computers and Electrical Engineering (2016), http://dx.doi.org/10.1016/j.compeleceng.2016.01.022