Computer Networks 88 (2015) 161–177

Contents lists available at ScienceDirect

Computer Networks

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

Location-dependent disclosure risk based decision support framework for persistent authentication in pervasive computing applications

Uthpala Subodhani Premarathne [a,*], Ibrahim Khalil [b], Mohammed Atiquzzaman [c]

[a] National ICT Australia (NICTA), RMIT University, School of Computer Science and IT, Melbourne, VIC 3001, Australia
[b] RMIT University, School of Computer Science and IT, Melbourne, VIC 3001, Australia
[c] School of Computer Science, University of Oklahoma, Norman, OK 73019-6151, United States

ARTICLE INFO

Article history:
Received 21 November 2014
Revised 11 May 2015
Accepted 8 June 2015
Available online 26 June 2015

Keywords:
Disclosure risk
Location
Authentication
Pervasive computing

ABSTRACT

In pervasive computing applications (e.g. electronic health records), the amount of information permissible to be shared or accessed by mobile users results in high disclosure risks. Obfuscation techniques are desirable in reducing the impact of disclosing confidential information but with a significant loss of utility of information content. Thus, accesses to confidential data by mobile users need to be controlled so as to minimize the disclosure risks. To achieve these requirements, we propose a novel location-dependent disclosure risk based decision support framework for persistent authentication and data access management. We have derived the location dependent identity based disclosure risks at record level and file level by using the search theory and entropy. We have experimentally evaluated our proposed model using multi-level security model and fuzzy sets. We have further proved that our proposed technique can significantly reduce the impact of common privacy attacks by performing a comprehensive security analysis. In conclusion, this research presents a novel location-dependent disclosure risk-based decision support framework persistent authentication and a pragmatic data access management approach for highly privacy-sensitive pervasive computing applications.

1. Introduction

Pervasive computing applications, such as mobile cloud computing (MCC), overcome the resource constraints of mobile devices in order to facilitate scalable and efficient services [1]. Mobility, offloading data storage and offloading computations open up vulnerabilities of malicious data misuses such as disclosure of confidential information. Therefore, location change is a vital aspect for ensuring secure data utilizations in pervasive applications (e.g. patient's health data [2]).

Authenticating users and controlling the data utilizations adaptively based on context changes enhance the reliability of pervasive computing applications. Authentication based vulnerabilities are rated among the most significant causes of privacy and security breaches in pervasive computing systems involving confidential data [3]. One time authentication of users do not effectively account for the potential vulnerabilities based on the contextual variations (such as location variations). So, it is important to consider authentication mechanisms that can be used to account for context variations. Existing solutions on continuous authentications use periodic validations without considering the privacy preservation. Therefore, in this paper, we address the issue of

* Corresponding author. Tel.: +61 414569698; fax: +61 99251835.
E-mail addresses: uthpalasubodhani.premarathne@rmit.edu.au, uthpalasubodhani@rmit.edu.au (U.S. Premarathne), ibrahim.khalil@rmit.edu.au (I. Khalil), atiq@ou.edu (M. Atiquzzaman).

http://dx.doi.org/10.1016/j.comnet.2015.06.002
1389-1286/

privacy preserving adaptive continuous authentications for sensitive data access management in pervasive computing applications.

Recently reported incidents on misuses of patient health data [4] over portable mobile devices remotely intrigues research on secure data usage based on location. Limitations of existing authentication techniques for dynamic user behaviors in authorizing privacy sensitive data access over portable mobile devices intrigues research on more reliable approaches for user authentications in pervasive applications. Therefore, it is important to consider location as contextual information in facilitating reliable data utilizations.

Significance of incorporating the location for persistent authentication in pervasive computing applications is apparent due to several reasons.

- Users may access privacy-sensitive data (e.g. personal health records) on mobile devices from different locations.
- Users may share privacy-sensitive data access over multiple mobile devices–susceptible to potential malicious data misuses.
- Users may have frequent access of data over long sessions–susceptible to session hijacking attacks due to the possibility of having multiple sessions over multiple mobile devices and also long session times without explicit re-authentications.

In this view, it is vital to validate the current location as a part of user authentication to be a trusted location to disclose sensitive data.

1.1. Motivational scenarios–access electronic health records (EHRs) in collaborative healthcare applications

EHRs are being increasingly used as efficient means to facilitate diagnosis and treatment in various emergency situation. EHR can be accessed by healthcare service providers, healthcare professionals, patients, insurance companies as well as some family members of a patient.

Example: As shown in Fig. 1, health information resources of two patients $P1$ and $P2$. The *privacy level* of each resource is shown. There are three different types of EHR information resources: images (I_i), prescriptions (P_i) and test reports (T_i) with different permissible activities and associated *privacy levels*: *HC*–high confidential, *LC*–low confidential. The location dependent disclosure risks for I_1 vary depending on the location. And based on the clearance levels and permissible secure locations for each role of each user determines the success of accessing an EHR information source depending on the location dependent disclosure risks associated. Two roles are: *Doctor* is able to access highly confidential data from locations $L1, L2,$ and $L3$, and the *Insurance Officer* can only access highly confidential data only from $L2$. Neither the *Doctor* nor the *Insurance Officer* can access data from $L4$.

Suppose, during an emergency situation, the *Doctor* needs to access the sensitive data files from $L4$. In order to ensure secure data utilizations location-dependent authentication and authorizations need to be enforced. So it is evident that the context plays an important feature in providing reliable data utilization management in pervasive computing applications.

1.2. Limitations of existing work

Risk of disclosure of information is the likelihood of violating the privacy of data by a malicious entity within the network or from outside.

Existing disclosure risk metrics [5,6] do not consider the contextual dependencies for estimating the potential privacy risks. Data de-identification and obfuscation mechanisms can preserve information privacy by lowering disclosure risk but with obvious loss of utility of the original information content [7]. The traditional view of preserving privacy aims to withhold information disclosure, increase information control and restrict information access [8]. Furthermore, privacy should have context-aware characteristics in order to encompass the salient features of the nature of activities in distributed collaborative systems [8]. Therefore, with the advent of multiple mobile devices (e.g. laptops, smartphones), in addition to the static privacy measures of data additional contextual factors, such as the location, are significant in preserving security and privacy for information access in pervasive computing applications.

For instance, MCC applications require more scalable and secure storage solutions [9]. A comprehensive survey has been done on augmented storage solutions for MCC applications [10]. Existing storage augmentation solutions of MCC applications, such as Pheonix, E-DRM, EECRS, offer high energy efficiency and context awareness in data storage and access management. These solutions offer restrictive access using strict policies such as write-once-read-many and do not validate the authenticity for each access request. The lack of authentication makes these solutions less secure in facilitating privacy-sensitive data access [10]. Strong password based authentications are proposed for pervasive applications [11]. However, dynamic user behaviors (e.g. location changes) cannot be accounted in such static credentials based authentications. RFID based location sensing can be used for authentications with minimum disclosure of user specific information [12–14]. However, due to the insufficiency of information related to dynamic user behaviors reliability of authentication decisions may not be ensured. Therefore, more robust context-dependent authentication techniques are necessary for pervasive computing applications to ensure secure data utilization management.

1.3. Research objective

Risk of sharing privacy-sensitive information in open systems (e.g. collaborative healthcare systems) includes the vulnerabilities of being stolen, lost and illegal trade. Location of data access is an important aspect in secure data usage. In this paper we investigate the use of location for persistent authentication of users in pervasive computing applications. The main research objective is to enhance the reliability by incorporating location dependent disclosure risk for persistent authentication in order to mitigate a set of known attacks in pervasive computing applications. Our novel contribution is a location dependent disclosure risk estimation