Electronic Commerce Research and Applications 13 (2014) 164–177

Contents lists available at ScienceDirect

Electronic Commerce Research and Applications

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

Trust assessment of security for e-health systems

Şerif Bahtiyar [a,b,*], Mehmet Ufuk Çağlayan [a]

[a] *Computer Networks Research Laboratory, Department of Computer Engineering, Boğaziçi University, Bebek, Istanbul 34342, Turkey*
[b] *Progress R&D Center, Provus Information Technologies, Sisli, Istanbul, Turkey*

ARTICLE INFO

Article history:
Available online 15 November 2013

Keywords:
Trust
Assessment
Security
Architecture
E-health

ABSTRACT

The expansive connectivity of emerging information systems has set the stage for pervasive access to healthcare services via e-health systems for selecting the best possible healthcare services. Emerging systems are expected to be highly dynamic open environments connecting diverse number of healthcare services and autonomous entities that are autonomous agents or software applications representing patients. Entities in such dynamic environments may have different security needs from e-health systems raising the challenge of trust computations regarding security. In this research, we proposed a trust assessment model of an e-health service from the viewpoint of an entity. The model contains a comprehensive architecture applicable to different types of entities, and a novel set of trust assessment metrics may be used to assess a specific property of a security system (i.e. partial metrics) or all properties (i.e. total metrics). The simulation based evaluation of proposed model in the context of a Hospital Online Appointment Service has shown that the proposed model provides better trust computation results than existing trust models for e-health systems. Furthermore, the entities are also able to assess the trust even with incomplete security information.

1. Introduction

E-health systems provide ubiquitous access to healthcare services by sharing patients data whenever necessary over an open environment like the Internet. Electronic Health Records (EHRs) improve communications between healthcare providers (Neubauer and Heurix 2011), such as medical insurance and dental insurance (Wu et al. 2012). From the clinical perspective, the communication can save lives in some emergency circumstances. Thus, e-health systems have been widely used to improve healthcare services in modern societies.

Since e-health systems handle personal data, individuals' EHRs may be subject to security and privacy attacks; yet majority of the e-health systems have significant weakness (Tejero and de la Torre Díez 2012). Revelation of information such as financial or other protected health information may result in socioeconomic losses for patients. This in turn may reduce patients' trust in e-health systems in open environments, and they may prevent ubiquitous access to their EHRs which may result in ineffective health care delivery and pose serious health problems especially during emergency situations.

Emerging e-health systems are expected to be connected in open environments that contain diverse number of healthcare services and autonomous entities. Here, an entity is an autonomous agent or a software application which represents a patient. As the diversity of services increases, trust[1] problems related to security issues become complex, such as trust establishment (Conti et al. 2011). Information security has been often discussed in the terms of authentication, confidentiality, integrity, and availability (Chivers 1994, Sun et al. 2008). On the other hand, trust has been investigated in various fields of science, such as philosophy and computer science (Hussain et al. 2006, Massa 2007). However, there is no consensus about trust issues.

The trustworthiness of an e-health service mostly depends on its security system (Samuel and Zaïane 2012). A security system is a set of security mechanisms that are implemented according to a security policy. A security policy can be described as a collection of rules that allow or disallow possible actions, events, or something related to security (Chivers 1994, Kagal et al. 2001, Li et al. 2007). On the other hand, a security mechanism implements security policies in the system.

* Corresponding author at: Computer Networks Research Laboratory, Department of Computer Engineering, Boğaziçi University, Bebek, Istanbul 34342, Turkey. Tel.: +90 2123597781; fax: +90 2122872461.

E-mail addresses: serif.bahtiyar@boun.edu.tr, serif.bahtiyar@provus.com.tr (Ş. Bahtiyar), caglayan@boun.edu.tr (M.U. Çağlayan).

[1] Trust is has various definitions in information systems, such as trust is the judgment expressed by one user about another user, often directly and explicitly, sometimes indirectly through an evaluation of artifacts produced by that user or her activity on the system (Massa 2007). In another definition, trust is the subjective probability by which an individual expects that another individual performs a given action on which its welfare depends on (Jøsang et al. 2007). These definitions shows that the term trust is defined differently even in the same context.

1567-4223/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.elerap.2013.10.003

Each entity has different trust perception factors regarding systems in open environments, such as security of e-health systems and e-commerce applications (Costante et al. 2011). Trust perception factors depend highly on subjective needs of an entity and social constraints. For instance, dental records of a patient may be private information for the patient because of insurance reasons or simply because of the perception of dental problems in the society. On the other hand, a patient may share his dental records because the records are not considered as private information by that patient. It is expected that patients may not be willing to disclose personal information more accurately or seek medical care for certain sensitive conditions if they cannot trust that their personal health information will be managed with high level of confidentiality (Avancha et al. 2012, Martí et al. 2013, Appari and Johnson 2010, Haas et al. 2011, Trcek and Brodnik 2013, Alemán et al. 2013). Actually, there are many researches and challenges on e-health security and privacy but the researches do not provide desired security level and the challenges still remain. Therefore, an entity may trust security system of e-health services according to its own needs and how it interacts with the services. The entity can make decisions for future interactions with the e-health services based on contextual needs and perceived trust. Generally, the entity may consider the security of an e-health system service and form trust before interacting with it. If an entity has higher trust on the security of e-health system, the entity will likely use the system more often which in turn may promote effective healthcare delivery and perhaps reduce healthcare costs. However, it would require trustworthy security of e-health systems (Zhang and Liu 2010). Therefore, assessing the trust of e-health system's security from the viewpoint of an entity is critical. Furthermore, such valuation necessitates specific trust assessment architectures of entities along with precise computational models.

Recently, several trust computational models have been proposed for various online business environments (Jøsang et al. 2007, Massa 2007, Yan 2007) that may be extended to assessing trust regarding the security of e-health systems. However, these trust computational models do not specifically provide solution to assess the trust from an entity point of view. Our research is motivated by this critical gap in that there is a need for trust model and trust assessment architecture for entities, where an entity can assess the trust of security of e-health system according to its own needs in the emerging open environment.

In this paper, we propose an entity oriented model for trust assessment of security of an e-health system. This model is flexible in its approach and facilitates an entity to assess the trust, using a novel set of trust assessment metrics, of all properties of a security system or some properties of the security system depending on the contextual need. Further, we demonstrate the applicability of the model and evaluate its performance in the context of a case study where the behaviors of proposed metrics are analyzed under several scenarios using simulations and compared with existing trust computation models. Our simulation results suggest the proposed model performs better than existing trust computation models. In summary, the primary contributions of our research are twofold.

- First, we introduced a novel trust assessment architecture accounting for complexity of health care delivery system and the diverse needs of an entity participating in the e-health system in emerging open environments.
- Next, we proposed two types of trust assessment metrics – partial metrics and total metrics – that offer flexibility to entity for assessing its trust level on the security system. The entity may assess either a specific property of security system (partial metrics) or all properties of the security system (total metrics) depending on the contextual needs. Subsequently, the entity may use only those security properties to which it has trust for its future interactions with the e-health system.

The rest of the paper is organized as follows. Section 2 provides a brief overview of e-health, trust and different trust computation models prevalent in the e-commerce and computer science literature. Section 3 describes our proposed trust assessment architecture followed by discussion of trust assessment metrics and trust assessment process in the Section 4. Finally, Section 5 presents a case study with a simulation based evaluation in the context of an Online Appointment Service of a hospital, followed by concluding remarks in the Section 6.

2. E-health, trust, and related issues

2.1. A brief overview of e-health systems

Healthcare organizations have changed their storage systems of health records from paper-based systems to electronic systems to provide better health care services, e-health services. Additionally, open systems like the Internet connect various e-health services (Mans et al. 2013) so service providers, such as doctors and hospitals, can share and access patients medical data remotely for increasing quality of care services (Masud et al. 2012). Therefore, Electronic Medical Records (EMR) or Health Information Systems (HIS) have been integrating in hospitals to improve the quality (Esposito et al. 2014). Actually, medical data about a patient are distributed among many e-health providers, such as different hospitals, laboratories, and doctors. An e-health system may integrate many e-health provides over different information systems to ensure access to such medical data. An abstract e-health system is shown in Fig. 1, which connects different e-health providers and e-health consumers.

Initial e-health systems had limited capabilities within certain departments of hospitals and clinics, such as Dental Information System for storing and managing dental-related data. The next step was integrating medical information systems of all departments to support information sharing in the hospital as a whole. For instance, Picture Archiving and Communication System (PACS) provides an integrated image management and communication system within departments of hospital (Esposito et al. 2014). Current trend in e-health systems is to combine fragmented hospital e-health systems to be able to share medical data for ensuring high quality care services. However, there are technical, sociological, and political problems regarding sharing medical data (Tawfik et al. 2012, Khan et al. 2013, Meo et al. 2011). Various countries and institutions involve in solving social and political problems about flow of medical information among different systems and providers. There are also many approaches to solve technical challenges of e-health systems (Aragues et al. 2011). As an example, framework architecture to cope with the challenge for fast deployment of e-health services is presented in (Fengou et al. 2013). Briefly, e-health domain is a multidisciplinary area that is influenced by different scientific fields.

2.2. Definition of trust

Trust is investigated in many fields of science, such as computer science, economics, politics, sociology and philosophy (Deutsch 1958, Grandison and Sloman 2000, Jøsang et al. 2007, Misztal 1996). However, there is no agreement about the definition and properties of trust (Gollmann 2006, Massa 2007, Raya et al. 2008). Trust is also defined in different manner in the same research field, such as in computer science (Jøsang et al. 2007, Raya