Computer Communications 31 (2008) 4060–4071

Contents lists available at ScienceDirect

Computer Communications

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

Cognitive agents based authentication & privacy scheme for mobile transactions (CABAPS)

B. Sathish Babu, P. Venkataram *

Protocol Engineering and Technology Unit, Electrical Communication Engineering, Indian Institute of Science, Bangalore, India

ARTICLE INFO

Article history:
Received 20 November 2007
Accepted 13 August 2008
Available online 26 August 2008

Keywords:
Mobile security
Authentication
Privacy
Mobile transactions
Cognitive agents

ABSTRACT

Maintaining anonymity during authentication has become challenging research issue in the field of mobile security. The application level authentication schemes have seriously affected by the absence of effective mechanisms to protect the privacy of a client transactions. We propose a novel Cognitive Agents Based Authentication and Privacy Scheme (CABAPS) for mobile transactions, which integrates procedure of authentication with privacy protection. The authentication challenges and privacy measures are dynamically deployed by cognitive agents based on transaction sensitivity and users behaviors. The method has been successfully simulated using the Agent Factory framework for cognitive agents generation and communication.

1. Introduction

Mobile communication and services over emerging wireless technologies provide anyone, anytime and anywhere access. Increased importance in mobile telecommunication and dominance of data communication promoted large segment of users to accept the mobile data communication as a part of their day-to-day activities. However, the wireless medium has certain limitations over the wired medium such as: open access, bandwidth insufficiency, computational restrictions, complex system functioning, power confinement, and relatively unreliable network connectivity. These limitations make it difficult to design efficient security schemes for authentication, integrity and confidentiality. Introduction of many value added services in mobile world, has triggered exorbitant growth of mobile users population, and many of these services demands a stringent authentication and privacy requirements to ensure that legitimate users are using the services with their privacy protected.

1.1. Mobile authentication and privacy

Authentication is a process to identify a mobile user (MU), in order to authorize him/her to use system resources for specified purposes, it involves negotiating secret credentials between prover and verifier for protecting communications. Privacy is a multifaceted term with many contextually dependent meanings, one aspect of the right to privacy is the right of an individual to decide for himself or herself when and on what terms his/her attributes should be revealed [1]. The cost cutting motive of the businesses in order to streamline the customer interactions, has increased the collection of personal information cheaply and unobtrusively. This will lead to situations where in which authentication systems increase requests for identification, facilitating record linkages and behavior profiling, which ends with invasion of privacy.

The way authentication systems collect, retain, and reuse personal information might affect privacy interests of the users. Following are some of the scenarios of privacy invasion during authentication: Demanding personal facts during establishing initial identifier. The records of individual actions (such as individual habits, timings, relationships, etc.) would be created without the notice of the user during execution of the authentication procedure. Personal information is exposed at multiple points and to multiple entities during the operation of an authentication system. Variety of individuals are allowed within one or more institutions to access the users identity and other authentication related data depending on where and how they are stored. The disclosure of a mobile users identity during the authentication process will make an unauthorized third-party to track the mobile user's movements and whereabouts, a powerful intruder may extend this to include a time-sequence to track a user over time.

While authentication systems can cripple privacy in some of the above mentioned ways, they can also be used in privacy-enhancing or privacy-preserving ways, primarily by securing personal data and preventing unauthorized access to the data. In this direction, it is advantageous to combine authentication and privacy with

* Corresponding author. Tel.: +91 80 22932282.
E-mail addresses: bsb@ece.iisc.ernet.in (B.S. Babu), pallapa@ece.iisc.ernet.in (P. Venkataram).

0140-3664/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2008.08.011

transactions. The behaviors exhibited by the users during transactions, and transaction sensitivity levels can be used to implement an efficient authentication and privacy scheme for mobile communications.

1.2. Cognitive agents

In the proposed scheme, we use intellective approach for mobile authentication and privacy management using a type of intelligent agents, called cognitive agents (CAs). These are the agents with high reasoning capability to solve complex real world problems which have high degree of dynamism. The reasoning capabilities enable the CAs to infer, rather than look up, its responses to percepts. CAs are often intentional, which means that their actions are motivated by specific goals and they store a symbolic representation of the world available. The CAs knowledge organization and deduction mechanisms are similar to human thinking, which includes knowledge quantifiers like behaviors, observations, beliefs, desires, and intentions [2–4]. A cognitive act can be one of the following three actions [5]: (1) Perceiving information in the environment; (2) reasoning about those perceptions using existing knowledge; and (3) acting to make a reasoned change to the external or internal environment.

The dynamism we are incorporating in the scheme at the level of service providing and capturing the behaviors of the users. In a desktop environment there is a consistency in the user behavior, seldom varies with the change of service he/she is using. But in mobile environment, the user behavior is highly volatile, it changes with service, device, network, distance, time, location, cost, etc. Therefore a signature/anomaly detection kind of schemes used in wired networks, can not be efficient in mobile systems. A rational approach based on behaviors of the users would work efficiently in identifying the correct principal in mobile application services. The proposed authentication and privacy scheme uses belief generation and analysis model to study the mobile user behaviors. Based on these, the security system grades the user and challenge him/her as per the deviation of their present and past behaviors.

1.3. Proposed authentication & privacy scheme for mobile transactions

The Cognitive Agents Based Authentication and Privacy Scheme (CABAPS) use two types of cognitive agents: the *mobile cognitive agent (MCA)* and the *static cognitive agent (SCA)*, which are secured with respect to their construction and inter agent communications. The SCAs creates MCAs and sends them to mobile nodes during beginning of the service usage. The MCAs periodically generates the beliefs over user transactions by observing various user behaviors, and sends them to SCAs. The SCAs performs sensitivity and privacy analysis over the transactions submitted by the user. The authentication requirements are dynamically generated, based on the sensitivity of mobile transactions and the beliefs deviation factor. At the same time, the privacy is handled by obtaining privacy policies from an independent trusted entity called the *Privacy Handler*. A challenge/response protocol based on belief deviation factor and transactions sensitivity is incorporated in the system.

1.4. Organization of rest of the paper

The rest of the paper is organized as follows: Section 2 gives some of the related works, Section 3 provides definitions and terminologies, Section 4 discuss the functioning of the CABAPS, Section 5 provides gives simulation procedure and results, and finally Section 6 draws conclusions.

2. Related works

A method suggested by D. Samfat [6], for providing identity privacy to mobile users during authentication use data aliases in place of actual identifiers. The main idea is to set up a chain of aliases by generating at each security transaction a random alias. Each alias is computed by using the preceding one and not the real identity of the user. But important limitation of the approach is computing aliases over all the types of mobile devices is practically infeasible.

The combined web/mobile authentication for secure web access control proposed by Al-Qayedi et al. [7], claims the privacy could be gained by restricting the web server hosted by a merchant to know only username/password and the identity number. The other information about an user are only known to the authentication server, which is a part of the mobile network service provider. Even though the proposed scheme alleviates the need of high end computation for generating aliases, still the private data has been stored in authentication servers, which could be later used for behavior profiling and other activities.

In adaptive privacy-preserving authentication in vehicular networks [8], Sha et al. address the requirement of adaptive privacy. They claim privacy is a user specific concept, some users are more serious about their privacy than others. Thus, the system should support multiple privacy degrees, and each user should be allowed to choose his own privacy degree. The authentication protocol should support the tradeoff between the privacy degree and resource utilization according to the users specific privacy requirements. The system works with assumption that the user is sufficiently knowledgeable to specify the required privacy degree, which is not true in all the cases.

Chen [9] has proposed, a new authentication scheme for accessing contents, services and applications in both mobile device and Internet. The services and applications are divided into four groups according to their importance: extremely confidential group, very confidential group, confidential group, and free accessible group. The authentication usage levels are used to access the items in each of the four groups. The scheme does not make any attempts to categorize transactions happening in a particular group as a result of this transaction based attacks are still possible, and it does not look into privacy aspects during authentication.

VMSoar: a cognitive agent for network security [10], proposes a cognitive agent based intrusion detection model. The main aim of the model is recognizing plans of users and what goal the user want to achieve, whether it is a threat to the security of system. It also claims to generate future expected behaviors of the user. This model is proposed for wired networks, and not suitable for mobile environment due to intensity of computation involved.

In our earlier work [11], we have developed a basic model on transaction based authentication scheme for mobile communication using cognitive agents. The approach deploys authentication scheme based on the transaction sensitivity and client's behaviors. Additionally the user behavior analysis by cognitive agents provides rational approach towards establishing the legitimacy or illegitimacy of the mobile client.

3. Definitions

In this section we provide definitions for important terminologies used in the paper.

3.1. Behaviors

The behaviors refer to the actions or reactions of a user while formulating and executing the transactions. The behaviors are de-