Available online at www.sciencedirect.com
SCIENCE DIRECT®
Computer Communications 29 (2006) 2308–2321
computer communications
www.elsevier.com/locate/comcom

Secure brokerage mechanisms for mobile electronic commerce

Oscar Esparza *, Jose L. Muñoz, Miguel Soriano, Jordi Forné

Department of Telematics Engineering, Universitat Politècnica de Catalunya, C/ Jordi Girona 1 i 3, Campus Nord, Mod C3, UPC, 08034 Barcelona, Spain

Received 1 August 2005; received in revised form 30 November 2005; accepted 3 March 2006
Available online 3 April 2006

Abstract

The possibility of making the Internet accessible via mobile devices has generated an important opportunity for electronic commerce. Nevertheless, some deficiencies deter a massive use of m-commerce applications. Security and easiness of use are unavoidable conditions. The use of brokerage systems constitutes an interesting solution to speed up the information delivery to the users. Moreover, brokers can use mobile agents to efficiently and easily perform the search and retrieval of commercial information in the Internet. Although the mobile agent technology is a very suitable choice for the m-commerce scenario, there are security issues that hinder its use. In particular, an important aspect that must be solved for the m-commerce scenario is the mobile agent protection from manipulation attacks performed by malicious hosts. The first part of this paper describes a mechanism to reach this protection. We describe how to use software watermarking techniques in the mobile agent to detect manipulation attacks, and how the broker can be used to punish the malicious hosts. Once an m-commerce site is selected by the user, an end-to-end secure transaction must be established. The transaction can use several protocols, from a simple secure TLS channel to send a credit card number until a sophisticated payment protocol. In any case, Public Key Certificates (PKCs) are required for these protocols. It must be stressed that certificates management is a heavy process and that clients in the brokerage scenario are usually resource-limited. For this reason, the best option is that clients delegate this task to the broker. Notice that the broker is a Trusted Third Party (TTP) and, in general, it is not resource-limited. Therefore, the broker is appropriate for storing and managing PKCs. The second part of this paper addresses this issue, with a particular emphasis in the certificate status management which is the most complex task of certificate management.

Keywords: Broker; M-commerce; Mobile agent; Public Key Certificates (PKCs)

1. Introduction

The access to the Internet by means of mobile devices potentially increases the number of users of e-commerce. For instance, one of the novelties of m-commerce is the possibility of attracting clients in the neighborhoods of commercial and/or service centers by providing them with the appropriate information in a short time. Unfortunately, there are some aspects that hinder a massive implementation and development of m-commerce services if they are compared to habitual e-commerce services. Most of these drawbacks are related to the particular characteristics of the wireless environment (usually less bandwidth, lower latency, less stability of connections, less predictable availability) and the inherent constraints of the mobile devices (less powerful CPU, less memory, limitations on power consumption, form factor of displays, etc.). Additionally, there are other security drawbacks that can appear in these wireless scenarios and that must be solved before using m-commerce applications massively [20].

The use of a broker between the wired and the wireless network can ease the access to web information from the mobile terminals, and it can also alleviate some of these security constraints. The main function of a broker is buffering and caching the information [21] in order to re-use it, and also sending useful data to mobile users in a predictive mode, reducing the overall data traffic in the wireless link. The solution presented in [26] was based on a broker with cache and proxy systems that delegates the information

* Corresponding author. Tel.: +34 934010972; fax: +34 934011058.
E-mail addresses: oscar.esparza@entel.upc.es (O. Esparza), jose.munoz@entel.upc.es (J.L. Muñoz), soriano@entel.upc.es (M. Soriano), jforne@entel.upc.es (J. Forné).

0140-3664/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2006.03.005

search and retrieval tasks to mobile agents. It also integrates in the broker the management of Public Key Certificates (PKCs) for securing end-to-end m-commerce transactions. Nevertheless, in that work neither the secure operation of mobile agents nor the PKC status management was addressed. In this article the authors summarize the improvements that must be performed over the broker scenario to improve the security of the system.

The rest of the paper is organized as follows: Section 2 reviews some typical issues of brokerage systems for m-commerce. Section 3 describes a solution to protect the search agents from manipulation attacks performed by malicious hosts, as well as the way to punish them. Section 4 deals with the PKCs management for securing m-commerce transactions. Finally, some conclusions can be found in Section 5.

2. Broker structure

This paper pretends to improve some aspects of the broker architecture which was previously presented in [26]. However, before introducing these improvements a short overview of this broker architecture is presented. This section also introduces some actual scenarios for brokerage systems. Later, some aspects about how to manage mobility can be found.

2.1. Broker functionalities

Fig. 1 shows a general view of the brokerage system. The broker acts as a mediator between the mobile users in the wireless network and the servers in the wired network (Internet). Mobile users can request for information or services in the Internet, these requests arrive to the broker, which creates a mobile agent programmed with some search patterns or service negotiation instructions. This mobile agent is sent to the Internet to perform the tasks on behalf of the user and, when finished, it returns to the broker. The results are sent back to the mobile user in a response message, and additionally the broker can store them in order to re-use these data in other requests. The broker must also provide access to a Public Key Infrastructure (PKI) to secure the end-to-end transactions with selected m-commerce sites when needed.

Fig. 2 shows the main functionalities of the broker, which are detailed below:

(1) Information search and retrieval: tasks such as searching, advising, contacting, comparing, filtering and facilitating access to databases perfectly fit for mobile agent technology [5]. In this sense, mobile agents can perform some tasks on behalf of a user while the mobile device remains off-line, which is very desirable on a noisy weak link with unpredictable disconnection.
(2) Intermediate storage: the broker stores a copy of the information that it receives. This allows the broker to re-use these data in the transactions of other mobile users. Accordingly, the information must be organized inside proxy and cache systems to ease and speed up its search into the broker.
(3) Customer Relationship Management (CRM): the knowledge of the user profile allows to manage the user's needs and wishes, and to deliver the services in a predictive fashion. The user profile can be managed and updated dynamically, depending on previous transactions or other external information sources. In particular, in the wireless environment CRM can profit from the facilities of the push mechanism of current mobile communications protocols.
(4) Certificate management: the access to a PKI is needed to provide most of the security services, such as integrity, privacy, authentication and access control. The broker can make lighter these tasks to the mobile users by storing and managing Public Key Certificates (PKCs) and the status of these PKCs.

This paper deals with the mechanisms that the authors propose to improve functions 1 and 4 to enhance the overall usability and security of the brokerage system. These mechanisms are discussed in Sections 3 and 4, respectively.

2.2. Actual scenarios

The IST-FP6 SIMPLICITY project founded by the European Union [1] works in an actual scenario for the broker architecture. The goal of this project is reducing the complexity of adapting systems beyond 3G by end-users and service providers mainly by: (1) providing

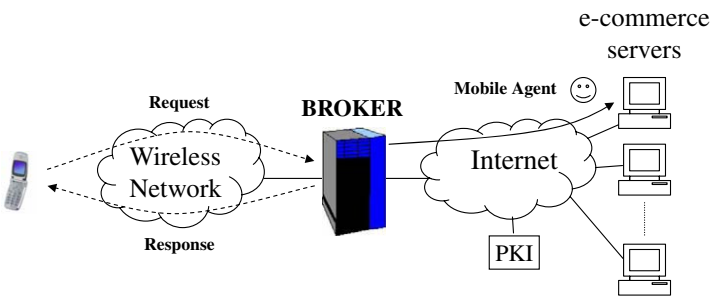

Fig. 1. Broker architecture.