Chapter XII

Remote Digital Signing for Mobile Commerce

Oguz Kaan Onbilger, University of Florida, USA
Randy Chow, University of Florida, USA
Richard Newman, University of Florida, USA

Abstract

Mobile agents (MAs) are a promising technology which directly address physical limitations of mobile devices such as limited battery life, intermittent and low-bandwidth connections, with their capability of providing disconnected operation. This chapter addresses the problem of digital contract signing with MAs, which is an important part of any mobile commerce activity and one special challenging case of computing with secrets remotely in public. The authors use a multi-agent model together with simple secret splitting schemes for signing with shares of a secret key carried by MAs, cooperating to accomplish a trading task. In addition to known key splitting techniques of RSA, authors introduce similar techniques for El Gamal and DSS public key cryptosystems. The objective is to achieve a simple and ubiquitous solution by using the well-known public-key cryptosystem implementations, which conform to the established standards.
Introduction

Mobile agents (MAs) are an approach to distributed computing employing the mobile code concept. An MA is an autonomous entity, which is composed of code, data and state information. They visit hosts (e.g., servers) possibly using an itinerary, perform some execution on those hosts using their codes and migrate with their state information from host to host. They act on behalf of their owners (i.e., senders). They are autonomous in the sense that they have all the knowledge needed to perform the assigned task on behalf of their owners.

Although the MA paradigm opens many interesting applications, to validate it as an alternative to traditional client/server computing, one must address its security issues. In particular, it should demonstrate the ability to compute with secrets in remote public domains. A good example of the need for this is digitally signing a contract for m-commerce (and in general e-commerce) applications with MAs as shown by Sander and Tschudin (1998). We call this problem remote digital signing. In this chapter, a multi-agent architecture is used and a solution to this problem is presented. The techniques we explore and analyze are based on information dispersal in distributed system security terms as well as multisignatures and secret splitting in cryptographic terms. The idea is to devise a secure way of sharing secret keys among members of a multi-agent group and signing with shares.

Electronic Commerce and Mobile Agents

Among many application areas of MAs (such as information retrieval, e-commerce, network management, network/site security, distance education, and software distribution), e-commerce draws the most attention from both academic and industrial researchers; for example see Busch, Roth, and Meister (1998) and Klusch (1999). This is mostly due to the fact that MAs and in general agent systems have the capability of representing users (i.e., customers) in the cyberspace. Agents can effectively profile user preferences, act on behalf their owners, participate in e-auctions, watch stock prices, search for commodities and find the best offer from competing vendors, purchase goods by paying and committing to transactions, communicate and cooperate with other agents of relevant goals. Although it is now agreed that MAs are not a new enabling technology, they offer many technical capabilities together (i.e., all-in-one) over the traditional client/server computing (Chess, Grosos, Harrison, Levine, Parris & Tsudik, 1995a; Chess, Harrison & Kershenbaum, 1995b; Lange & Oshima, 1998). Mobile commerce (m-commerce), which is a rapidly growing field in e-commerce, is especially a suitable application area of MAs.

Mobile Commerce and Mobile Agents

Mobility of agents brings unique advantages to m-commerce. Mobile devices such as PDAs and laptop computers have limited battery life, intermittent and low-bandwidth...
What Predicts Commercial Bank Leaders’ Intention to Use Mobile Commerce?: The Roles of Leadership Behaviors, Resistance to Change, and Technology Acceptance Model
www.igi-global.com/chapter/predicts-commercial-bank-leaders-intention/74522?camid=4v1a

Factors Affecting Users’ Release Behavior Intention Based on WeChat Innovation Platform: An Exploratory Study
Wanxin Xue, Yilei Pei, Dandan Li and Yi Li (2017). *Journal of Electronic Commerce in Organizations* (pp. 72-82).
www.igi-global.com/article/factors-affecting-users-release-behavior-intention-based-on-wechat-innovation-platform/188838?camid=4v1a