A mobile agent is an autonomous software program, which can be executed in different agent platforms for a specific task on behalf of a customer. Furthermore, a mobile agent has the mobility to travel from one host to another in the world of network systems. Besides, mobile agent technology is suitable for reducing the computational overhead of a local host and providing low cost of communications. Thus, the characteristics of mobile agents, autonomy and mobility, make them ideal for e-commerce applications. In the past few years, e-commerce has become flourishing and rising in most enterprises. The benefit of employing the mobile agent technology in the enterprises allows deployment of e-commerce services in a more flexible and customizable way. Moreover, it improves the competitive advantages and the efficiency of organizational operations. However, the explosion of e-commerce is forcing businesses and customers to focus on developing a secure transaction environment on Internet. Therefore, the security is one of the key issues for mobile agent technology while the mobile agents are applied to the developments of e-commerce. In order to protect the security of transactions in e-commerce, this thesis proposed an appropriate public key cryptosystem for the mobile agent based networks. The proposed cryptosystem is constructed by using the pairing-based cryptosystems, and is developed by integrating the identity-based public key cryptosystems with the self-certified public key cryptosystems. In addition, we further employ the integrated cryptosystems to design several security schemes for the mobile agent based networks. As far as mobile agent security is concerned, we devise a new proxy signature scheme, undetachable proxy signature, which is combined with the advantages of undetachable signature and proxy signature to protect mobile agents. We also develop a proxy authenticated encryption scheme to satisfy the basic security requirements of confidentiality, integrity, authenticity, and non-repudiation for mobile agents. As far as agent platform security is concerned, we apply the idea of proxy signature to construct a single sign-on (SSO) scheme for agent platforms. This scheme is based on the proposed cryptosystem to achieve the requirements of authentication and authorization. In summary, the proposed security schemes can make the mobile agent environments securely workable.

Keywords: mobile agent, proxy signature, authenticated encryption scheme, single sign-on, self-certified public key cryptosystems, pairing-based cryptosystems


Chien-Lung Hsu, Authenticated Encryption Schemes for Group Oriented Applications, Ph.D dissertation, National Taiwan University of Science and Technology, Taiwan, 2002.


