Application of Mobile Agent and Cryptography For The Security of Job Applicants on Mobile Phones

Ei Khaing Win, and Mie Mie Su Thwin

Abstract— Job search and application is not a new area and several significant works have been done to modernize, improve security and increase the success and usage of these systems. Nowadays, due to the proliferation of mobile devices, they are widely used to access information, search and apply jobs in large hostile networks like internet anywhere and anytime. However, mobile users have to come across the problems like frequent disconnection and high error rates in wireless environments. To solve these problems, the Mobile agent technology and Web Service technology are integrated. Due to the security issues in Mobile agent technology, it is also very important for both of job search sites and applicants to face the challenges towards security concerns in the job application process. As security is a major concern, it is very important that the data should be protected by using cryptographic techniques. In this paper, we propose the system that incorporates the mobile agent, web service and certificateless cryptography for the security of job applicants in wireless environments.

Keywords—Certificateless Cryptography, Job Application Process, Mobile Agent, Mobile Devices, Web Service

I. Introduction

EFFICIENT execution of wireless applications is of paramount importance due to the highly dynamic wireless network conditions. The requirement for ubiquitous service access in wireless environments presents a great challenge in light of well-known problems like high error rate and frequent disconnections [2].

Web services specification provides an open standard for the distributed service oriented architecture. Software components that can be published, located, and run over the Internet using Extensible Markup Language (XML).Web services allow other applications to call modules of code remotely with XML and applications can be built that are platform-independent, distributed and secure [1].

A mobile agent is a composition of computer software and data which is able to migrate from one host to another autonomously and continue its execution on the destination host. While mobile agents approach provides a great flexibility and customizability compared to the traditional client-server approaches, it introduces many serious security problems.

These problems are mainly protecting the hosting server and the visiting agent from each other. Currently, Web services and mobile agent security is mostly based on Certification Authorities (CA) based public key infrastructure and identity-based cryptography [1].

This paper introduces a new security control scheme for the integrated mobile agent and web service Technology based on certificateless cryptography and key agreement protocol.

II. Related Work

The applications combining of mobile agents and web service technology have drawn much attention in recent years.

Dominic Cooney et al. presented a model for implementing Web services with mobile agents [11]. Jan Peters introduced integration architecture of mobile agents and web services [12].In [2], a framework for the implementation of semantic web services and mobile agent integration for efficient mobile services was proposed. However, security schemes for combination schemes of mobile agents and web services were not considered.

Mobile agent and web services security is still of a big concern for some applications. Web services and mobile agent security is mostly based on Certification Authorities based public key infrastructure.

In [1], a security scheme for mobile agent and web service integration was proposed. The security architecture employed identity-based public key system and provided a new authentication protocol without using username/password pair. It gave an alternative method to current security mechanism without using Certification Authorities based public key infrastructure. Moreover, trusted third party was not required as the security was handled by a particular web service provider where a specific service was offered and identity-based cryptography is designed only for closed organizations.

However, in some applications in which a person wants to seek a job, job seekers will not know many web service providers in advance. In this case, Online Career Center is required as trusted third party for securely interacting with the service providers. Protecting the job applicant's identity and salary negotiation information is not only important but also necessary to find job offers more effectively. So it must be protected from third party and information must only be known by job seeker and web service provider. Trusted third party is only required for first time interaction of job applicant and web service provider.

Ei Khaing Win, Faculty of Information and Communication Technology ,University of Technology (Yatanarpon Cyber City), Pyin-Oo-Lwin, Mandalay, ekwdhnin@gmail.com

Mie Mie Su Thwin, Myanmar Computer Emergency Response Team, Ministry of Science and Technology, Yangon, Myanmar, miemiesuthwinster@gmail.com