SEC: Security Control System for the Integration of Mobile Agent and Web Services based on Certificateless Cryptography and Two Party Hashing Key Agreement Protocol

Ei Khaing Win[*], Mie Mie Su Thwin[I]

[*]*Faculty of Information and Communication Technology*

[*]*University Of Technology (Yatanarpon Cyber City)*

[*]*Pyin Oo Lwin, Myanmar*

[*]ekwdhnin@gmail.com, drmiemiesuthwin@mmcert.org.mm[I]

Abstract

Security is a major concern for wide applications in large hostile networks like internet. More and More people are willing to access information anytime and anywhere. The advances in mobile devices and wireless networks lead to requirements to tackle the problems like high error rates and frequent disconnections. Currently, the two modern technologies: Mobile Agents and Web Services are used altogether to achieve ubiquitous service access. As a result of applications using combination of mobile agent and web services, security becomes a big concern for applications. The integration of mobile agent and cryptography technologies provide benefits such as improved accessibility wirelessly and increased security. In this paper, SEC (Security Control) System to control the security of the integrated Mobile Agent and Web Services based on certificateless cryptography and (TPHK), two party hashing key agreement protocol, is proposed.

Keywords— mobile agent, web service, certificateless cryptography, key agreement protocol, security control system

1. 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.

2. 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