Security Control System for the Integration of Mobile Agent and Web Services based on Certificateless Cryptography and Key Agreement Protocol

Ei Khaing Win[*], Mie Mie Su Thwin[I]
[*]*Faculty of Information and Communication Technology*
[*]*University of Technology (Yatanarpon Cyber City), Myanmar*

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. Mobile Agent technology is applicable to devices with limited bandwidth and computing resources and long-term transactions without constant interactions. Web Services are an emerging technology that provides interoperability between applications running in different platforms. 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, the job search system for mobile phone users is proposed .The problems encountered by mobile phone users like frequent connection loss and security issues can be overcome by using the combination of Mobile Agent and appropriate cryptography technique, certificateless cryptography. The solution may therefore be ideal in a wireless environment or in low-power devices where resources are limited. Moreover, (TPHK) two party hashing key agreement protocol is also proposed to save communication costs with third parties each time and to securely establish a common secret key preventing an undesired third-party from injecting any weak keys on the agreeing parties.

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 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.

In this paper, the security scheme for the integrated Mobile Agent and Web Services based on certificateless cryptography and key agreement protocol is proposed.

3. Mobile Agent

A mobile agent is a software agent that has the ability to transfer its program code, data and execution state across a network to a remote computer for execution.

Mobile agent systems have many advantages over traditional (static) distributed computing environment.

- require less network bandwidth
- increase asynchrony among clients and servers
- dynamically update server interfaces
- introduce concurrency [6].

Generally security issues in mobile agents as

- Protection of the host from malicious code
- Protection of the agent from a malicious host trying to tamper the code and the agent data [10].

Mobile agent security technique based on encryption hide the mobile agent, code, or sensitive data so that it cannot be recognized and thus will be less likely to be destroyed, stolen, or otherwise misused [9]. The integrity of the data collected by a mobile agent might be protected using a cryptographic technique [5].

4. Web Services

Web services are software components built upon Web-based technologies including HTTP and XML and allow standard means of interoperability over the Internet of intranets between application running on a large variety of hardware and platforms [8].

5. Security Issues in Web Services and Mobile Agent System

The data transmitted between mobile agent and web service may contain sensitive data. The requirement to meet the issues is confidentiality, authentication, authorization, integrity and non-repudiation [1].

Confidentiality means the protection of data from unauthorized disclosure. And this can be achieved through encryption. Authentication is the assurance that the communicating entity is the one that it claims to be. Authorization is the ability to decide if person, program or device is allowed to have access to data, functionality or service. Integrity is the ability to detect if information is tampered with, it can be detected. Non-repudiation is the ability to verify that the sender and recipient were the parties who claimed to send or receive the message respectively [8].

6. Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. Most common systems use a public key cryptography system.

6.1. Public-Key Cryptography

It is the most popular solution for proving authenticity of public keys. It allows parties to set up secure transmission channel with no prior exchange of secret keys. Each user generates a pair of keys called public and private key. The former is used for encryption and the latter for decryption.

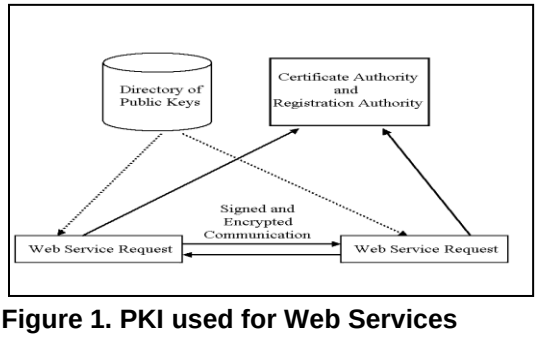

Figure 1. PKI used for Web Services

Public-key infrastructure (PKI) proves authenticity of users' keys by means of certificates. Firstly, key pairs are generated for the user and Web service provider and public keys are registered with the registration authority. The certificate authority (Trusted Third party or "TTP") issues a digital certificate with the public key. Secondly, the Web services user can retrieve the public key of the Web services provider from a PKI directory. Finally, the Web services provide can communicate securely with key pair [1].

But there are some drawbacks when PKI are applied in web services. Namely, all the users must have his/her public/private key pair based on PKI, and the service server must verify and manage all users' public keys. In addition, the service server has to search the user's public key and use different keys to encrypt messages for different users whenever they send the message to the user [3].

6.2. Identity-Based Cryptography

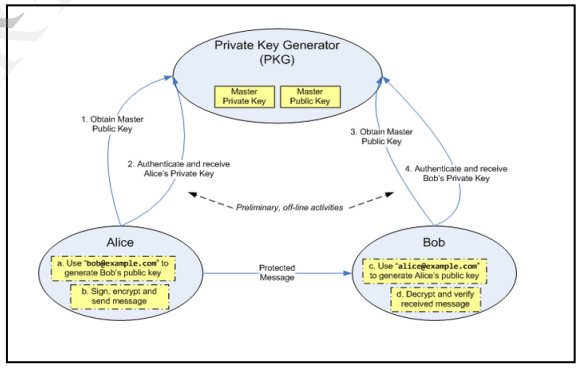

Figure 2. ID-based Encryption Steps

Identity-based cryptography is a type of public-key cryptography in which a publicly known string representing an individual or organization is used as a public key. The public string could include an email address, domain name, or a physical IP address. ID-based encryption (or Identity-Based Encryption (IBE)) is an important primitive of ID-based cryptography. It enables sender to encrypt a message when the only information she knows is recipient's identity (e.g. email address).Additionally, users do not need certificates to bind identity with specific public key. There is a trusted party called a *private-key generator* (PKG) which performs the system setup, generates a secret called the

master key and provides private keys to clients using it. But it also has its own drawbacks. A new Web Services and mobile agent system confidentiality protocol, which provides an alternative method to current security mechanisms without using Certification Authorities (CA), have been proposed to simplify the key management and reduce the computation load by using the ID-based authentication scheme.

As the PKG computes a private key for a client, it can decrypt all of her messages passively. This inherent key escrow property asks for complete trust in the PKG, which is difficult to find in many realistic scenarios. Trust placed in PKG is very high since it works as a key escrow and is capable of decrypting all the traffic. This property eliminates original IBE scheme from wide applications in big hostile networks like the Internet [1]. However, it is still usable in closed commercial environments. To solve the key escrow problem, security architecture using certificateless cryptography can be used.

6.3. Certificateless Cryptography

It is an interesting alternative to traditional PKI. It makes use of identities, which are users' public keys formed of arbitrary strings, in place of certificates. Besides, it's infrastructure is lightweight and can be deployed at much lower cost. Moreover, it offers transparent encryption, so that non-technical users could easily secure their data. It may be employed to provide transparent email encryption, which is desirable in real-world security applications. It is a promising solution improving several weaknesses of public key infrastructure and identity-based encryption [3].

7. Motivation and Current Status of the System

Currently, Web services and mobile agent security is mostly based on Certification Authorities (CA) based public key infrastructure. And identity-based security scheme has been proposed without the participation of trusted third party. However, in communicating two parties that have not known each other, the participation of trusted third party is necessary for non-repudiation and for the authenticity of users' public keys. However, total trust in key generation centre leads to problems in security. It is more desirable that KGC involves only in the key generation of participants. And exchange of messages can only be performed by the two parties without the intervention of KGC. Moreover, some web service providers have resources that are given access to particular user group.

- Stronger Confidentiality: Maintaining confidentiality by only one session key can be risky. The compromise of that key can easily break the system. In order to protect the system from adversary who compromises session key, the security of the system is further maintained by another session key for stronger confidentiality.

- Easy management of users: Users can be easily managed by informing the newly generated group session key to user via email. Membership management can be handled by regenerating group session key.

- Reduce Load of Users: Users do not need to regenerate their session keys. They only need to check the latest group session key via email.

8. System Architecture

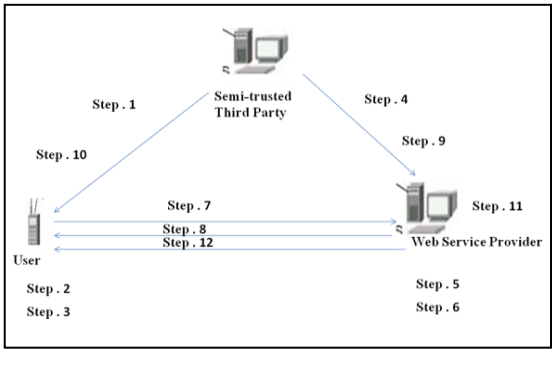

Figure 3. System Flow

Step 1: Mobile User firstly obtains partial private key and public parameters generated by Semi-trusted Third Party.

Step 2: User create private key by using partial private key and its secret value.

Step 3: Then user create public key using public parameters, its ID and secret value.

In a similar fashion,

Step 4: Web Service Provider obtains partial private key and public parameters from Semi-trusted Third Party.

Step 5: Then, private key is created using partial private key and its own secret value.

Step 6: Public key is also generated using public parameters from Semi-trusted Third Party, ID and secret value.

Instead of using certificateless cryptography, key agreement is performed to save communication costs. As a result, two parties can communicate without the intervention of third parties next time.

Key Agreement between User and Web Service Provider

Step 7: User sends its ID, public key, random numbers and mail-ID to web service provider.

Step 8: Similarly, web service provider sends its ID, public key, random numbers and mail-ID to user.

Step 9: Web Service Provider generate session key using keys obtained from user and its own ID, public key, random numbers and mail-ID.

Step 10: User also generate session key using keys sent by web service provider by combining its own ID, public key, random numbers and mail-ID.

Step 11: Web Service Provider then generate group session keys for users who can access particular resource.

Step 12: That group session key is then sent to the users via email.

After making key agreement between mobile user and web service provider, data can be encrypted and exchanged using mobile agent.

In Job Search System, Online Career Center takes the place of Semi-trusted Third Party. Several job service providers join it and create their own private keys. In a similar style, job seeker using mobile phone must first join the Online Career Center and then get information about several job service providers. Then he communicates with specific service providers securely without the intervention of Third Party by creating TPHK. In this way, job information such as the job applicant's identity and salary negotiation information can be protected from unauthorized parties.

8.1. TPHK Key Agreement Protocol

Key agreement (KA) is one of the fundamental cryptographic primitives. It allows two or more parties to establish a secret key over open networks; each party can encrypt any message such that only the parties sharing the secret session key can decrypt the message [4].

User A sends his ID, public key, random number, mail-Id to web service provider B. Web Service Provider B sends ID, public key, random number, mail-Id to user A.

1. Key =H2(ID_A,ID_B,P_A,P_B,R_A,R_B,rP,e_{IDA},e_{IDB})
2. Key= H2(ID_A,ID_B,P_A,P_B,R_A,R_B,rP,e_{IDA},e_{IDB})

ID_A =ID of User A
ID_B= ID of Web Service Provider B
P_A= public key of User A
P_B= public key of Web Service Provider B
P= generator chosen from cyclic group G_1 where G_1 is an additive group having a prime order q.
$R_A=r_AP$ where $r_A \in Z_q$.
$R_B=r_BP$ where $r_B \in Z_q$.
e_{IDA} =Mail Id of User A
e_{IDB} =Mail Id of Web Service Provider B

8.2. Generate Group Session Key

Key=H2 (e_{ID1}, e_{ID2}, e_{ID3}, e_{ID4}, R_1)

The group session key for users 1,2,3,4 for Resource R_1 is generated. If user is no longer permitted to access resource1, then new group session key is generated and inform the authorized users via email.

8.3. Encryption

$E(P_{user},E(K_G,E(K_s,Msg)))$

Message is encrypted by using session key and then encrypted by using group session key and finally encrypted by using public key of the receiver.

9. Expected Contributions

This paper intends to propose robust security scheme for the integrated mobile agent and web service technology. And the scheme can protect against unauthorized third parties and it does not need to depend totally on Third parties. It can overcome the weakness of the wireless environment as frequent connection losses. Stronger Confidentiality can be gained. Moreover, authorization for the resource can easily be used for the confidentiality of the data.

10. Conclusion

The proposed system solves key escrow problem. Key escrow problem means that trusted third party can decrypt all of the messages of both parties as it knows all private keys. And it will satisfy the requirement like frequent disconnection in wireless environment. Moreover, users have less tension about management of their session keys. The confidentiality of data can be further promoted. And trust placed in key generator can be low.

11. References

[1] Junqi Zhang, Yan Wang and Vijay Varadharajan, "*Mobile Agent and Web service Integration Security Architecture*"
[2] Vasileios Baousis , Vassilis Spiliopoulos , Elias Zavitsanos , Stathes Hadjiefthymiades , Lazaros Merakos , "*Semantic Web Services and Mobile Agents integration for efficient Mobile Services*".
[3] Dr inz. Artur Krystosik ,"*Certificateless Cryptography* "
[4] Lei Zhang, Futai Zhang,Qianhong Wu, Josep Domingo-Ferrer, "*Simulatable Certificateless Two-Party Authenticated Key Agreement Protocol*"
[5] Sergio Loureiro, Refik Molva, Yves Roudier, "*Mobile Code Security*".
[6] Aneta Zwierko, Zbigniew Kotulski, "*Security of mobile agents: a new concept of the integrity protection*".
[7] William Stallings, "*Cryptography and Network Security*".
[8] Alin COBARZAN, "*Consuming Web Services on Mobile Platforms*".
[9] S.Greenerg Michael, C.Byington Jennifer, G.Harper David, "*Mobile Agents and Security*".
[10] G.Geetha, C.Jayakumar, "*Trust Enhanced Data Security in Free Roaming Mobile agents Using Symmetric Key cryptography*", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.
[11] D.Cooney and P.Roe. "*Mobile agents make for flexible web services*".In proceedings of The Ninth Australian World Wide Web Conference.Quensland, Australian, July, 2003.
[12] J.Peters. "*Integration of mobile agents and web serives*". In The First European Young Researchers Workshop on Service Oriented Computing (YR-SOC 2005), April 2005.