# Secure Internet Applications Based on Mobile Agents

Cungang Yang
Department of Electrical and Computer Engineering
Ryerson University, Toronto, Ontario, M5B 2K3, Canada. (Email: cungang@ee.ryerson.ca)

*(Received Aug. 22, 2005; revised and accepted Oct. 11 & Oct. 14, 2005)*

## Abstract

The increasing importance of the Internet has motivated the exploration of new execution models based on mobile and dynamic entities to overcome the limits of the client/server model traditionally used to develop Internet applications. In this research, an Enhanced Role-based access control model (ERBAC) and an architecture for the ERBAC model are proposed. The architecture based on mobile agents will be a suitable approach to achieve both security interoperation and privacy protection in the Internet environment. The significant of this method is that mobile agents tend to execute the information locally therefore reducing network traffic and latency. In addition, mobile agents make it feasible to automatically realize the security and privacy protection for Internet applications.

*Keywords: Digital credential, E-Commerce, ERBAC, mobile agents, RBAC*

## 1 Introduction

The Internet is an open and distributed system that interconnects heterogeneous nodes and networks. It has brought an enormous advance in permitting access to a large variety of data and in enabling a large number of activities to have a global reach [10]. While the Internet offers significant opportunities, the most serious problems faced by Internet architectures are their lack of security and privacy. Role-based Access Control model (RBAC) [16] is a security technology that is attracting increasing attention in recent years. The central notion of the RBAC model is that users do not directly get access to enterprise objects; instead, access privileges of the objects are associated with roles, and each user is assigned to one or multiple members of appropriate roles. As a result, an organization not only preserves access control policy appropriate to its characteristics consistently, but it also maintains access control relationships between users and objects independently. The key benefits of RBAC are simplified systems administration and enhanced systems security and integrity [18]. However, the fundamental RBAC model is only designed for a single enterprise domain, it is not concerned with the security and privacy problems for large distributed system, such as the Internet.

In this paper, a completed modeling and implementation of an Enhanced Role-based Access Control model (ERBAC) is introduced. In order to deal with the security problem of ERBAC model on the Internet, it is required to establish a trust relationship between the strangers in the Internet. Since digital credentials [1, 3, 4] can be used to manage trust establishment more efficiently, therefore digital credentials are introduced for Internet applications. Digital credentials are the online counterparts of paper credentials that people use in their daily lives, such as the credential of an ACM member, the credential of a medical doctor, etc. They are signed by CA (Certificate Authority) issuers and can be made verifiable and unforgeable. Recently, researchers have presented a complete automated trust negotiation strategy [17, 19, 22] by exchanging digital credentials between the strangers on the Internet. However, this security solution leads to privacy problems, digital credentials make them easy to collect and disclose too much personal private information. Thus, the goal of this research work will be focused on the modeling privacy requirements and the implementation of the ERBAC model for Internet applications.

The significance of the research work is that:

1) ERBAC model extends the original RBAC model from an enterprise domain to the Internet environment and deals with both security and privacy issues much more efficiently.

2) The architecture of the ERBAC model protects the data of digital credentials from hosts and mobile agents.

3) The proposed XML-based privacy policy is extensible, the enforcement of the policy is easy, and the modification of the policy is implemented automatically.

This paper is conducted at several different levels: The modeling privacy requirement in ERBAC model is de-

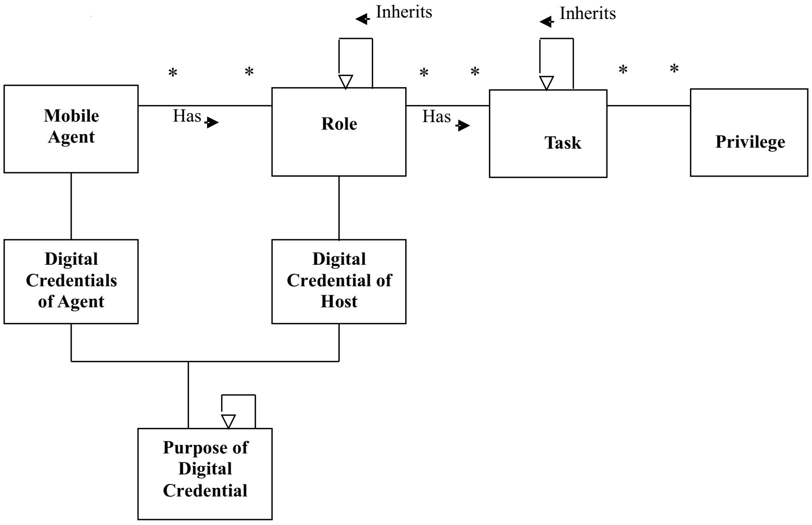
Inherits
Inherits
*
*
*
*
*
*
Mobile Agent
Has
Role
Has
Task
Privilege
Digital Credentials of Agent
Digital Credential of Host
Purpose of Digital Credential

Figure 1: Class diagram of the enhanced role-based access control model

scribed in Chapter 2, designing XML-based privacy policy for hosts and mobile agents is proposed in Chapter 3, developing the architecture of ERBAC model with mobile agent is introduced in Chapter 4, and the conclusion is presented in Chapter 5.

## 2 Modeling Privacy Requirements for ERBAC Model

Privacy is the right of individuals to determine for themselves when, how, and to what extend information about them is communicated to others [14]. It has been an increasing concern in the Internet applications. Traditional security models, such as Access Control Lists (ACL) and Mandatory Access Control (MAC), are not designed for enforcing privacy policies. The proposed Object-Oriented Role-based Access Control model (ORBAC) [20, 21] for web-based applications also cannot be used to enforce privacy policies because it was not designed to model purpose, the key element in privacy policies.

In the proposed ERBAC model shown in Figure 1, mobile agent is a program that can exercise a user's or organization's authority, work autonomously toward a goal, and meet and interact with host. Role is defined as a collection of tasks performed by mobile agents who are members of certain digital credentials. The reification of roles provides a convenient way to represent the notion of purpose [9], role is directly related with tasks, thus a certain responsibility was assigned and purposes of the role are represented. Role hierarchy represents the inherit relationships among the roles. A role inherits the tasks of its child roles. Task serves as an intermediary entity between roles and privileges and task hierarchy represents the inheritance relationships among the tasks. Each role may have multiple tasks and the same task can be assigned to multiple roles. The introduction of task and task hierarchy in ERBAC model not only satisfy the least of privilege principle and the privacy requirement of the system but also further simplifies the management of privacy policy. Privilege in the model is an access mode that can be accessed by roles, a role may have one or multiple privileges and a privilege can be assigned to one or multiple roles. To implement basic privacy principle, an important component, purpose, is introduced in the ERBAC model. Purpose structures the intended use of collected data into categories. Any good privacy practice always tells the customer how the collected data will be used. For example, the data may be used for marketing or for fulfilling the individual's order.

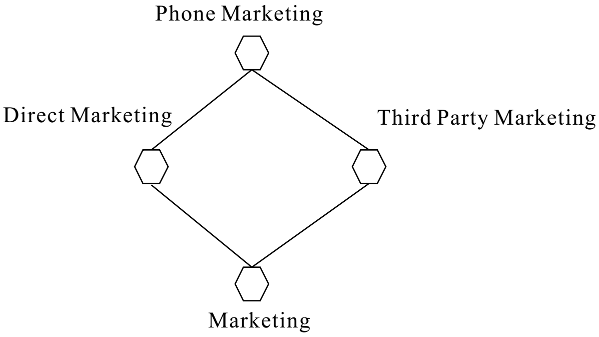

Figure 2: Example of purpose hierarchy

The relation between purposes can be modeled with a purpose hierarchy. The purpose relation is a partial ordered relation and partial ordered relations support complex purpose hierarchies. Different levels of purpose hierarchy is used to map high-level purpose to its low-level purposes. If an operation is allowed for a given purpose, it is also allowed for all its higher level purposes. An example of purpose hierarchy is shown in Figure 2 where the purposes of direct marketing and third-party marketing are specializations of the marketing purpose and phone marketing is specializations of (higher level) purpose of direct marketing and third party marketing. A principal assigned to purpose direct marketing (or third-party marketing) will inherit privileges assigned to the more general purpose of marketing. Data in agent's or host's digital credential has its own purpose level that expresses some conditions that should be satisfied before the data is able to be accessed. The level of the purpose of certain data in agent's digital credential is used to protect the privacy of the data in the agent's digital credential, while the level of the purpose of host's digital credential is used to protect the privacy of certain data in the host's digital credential. Moreover, agent and host also provide their purpose in order to access the data in the digital credentials. Agent and host share an equivalent purpose hierarchy, whenever an agent or host would like to access the data in the host or agent's digital credential, the purpose level of the agent or host should be presented and compared with the purpose level of the data in host or agent's digital credential. Based on the above analysis on the relationships among agent, host and purpose hierarchy, it is easy to conclude that the agent or host is allowed to access the data in host's or agent's digital credential only if the purpose level of host's (agent's) is greater or equal to the purpose level of the data in the agent's (host's) digital credential. For instance, in Figure 3, assume that the purpose level of agent A is " Direct Marketing", purpose level of data 1 in host's digital credential is "Third Party Marketing", purpose level of data 2 is "Phone Marketing" and purpose level of data 3 is "Direct Marketing", then it is concluded that only data 3 is allowed to be accessed by agent A. If we consider the case that host is getting access to the data in the agent's digital credential, the situation is the same as the agent.

# 3 Designing XML-based Privacy Policy

In this research, based on the privacy requirement of the ERBAC model, a privacy policy is proposed to formalize the ERBAC model and express restrictions on the access to the personal data of agent or host's digital credentials. The driving motivation of this effort is to simplify privacy policy administration for Internet applications. The privacy policy defines the syntax of the following element of the model: roles, mobile agents, tasks, privileges, digital credential of agent and its purpose hierarchy, digital credential of host and its purpose hierarchy. In addition, the privacy policy defines the syntax of the relationships among those elements.

There are two different approaches that could be used to formalize the privacy model: XML or the logical framework of the Authorization Specification Language (ASL) [15]. Our research intends to employ XML-based technology for privacy policy definition and representation because, as a meta-language, XML can effectively define ERBAC security policies and is able to be extended and modified easily. Also, XML represents desired privacy policies precisely and effectively and offers an additional degree of flexibility. Using XML-based technology, privacy policies for hosts and mobile agents are defined in Subsections 3.1 and 3.2.

## 3.1 XML-based Privacy Policy of Host

The privacy policy of host includes the following two parts: (1)<! − − Basic Elements − − > defines basic elements of the model including privilege, role, host credential, purpose hierarchy of host and task; (2)<! − − Relationships of Elements − − > defines the relationships between different elements of the model. (i.e. a role hierarchy associates a role with its direct child roles, privilege assignment assigns a set of privileges to a task, task assignment assigns a set of task to a role, etc.)

Based on the specifications of the XML-based ERBAC privacy policy, an example of a privacy policy of host is shown below:

**Example 1: (XML-based ERBAC Privacy Policy of Host)**

```
< ? xml version = "1.0" >
<ERBAC-MODEL TYPE = "PRIVACY_POLICY">
 <! − − Basic Elements − − >
   <! − − Privilege definition− − >
     <PRIVILEGE ID = "O1"> < /OBJECT>
     <PRIVILEGE ID = "O2"> < /OBJECT>
     <PRIVILEGE ID = "O3"> < /OBJECT>
     <PRIVILEGE ID = "O4"> < /OBJECT>
   < / − − Privilege definition− − >
   <!− Role definition− − >
     <ROLE ID = "R1"> < /ROLE>
     <ROLE ID = "R2"> < /ROLE>
     <ROLE ID = "R3"> < /ROLE>
     <ROLE ID = "R4"> < /ROLE>
   < /− Role definition− − >
   <!− Task definition− − >
     <TASK ID = "T1"> < /TASK>
     <TASK ID = "T2"> < /TASK>
     <TASK ID = "T3"> < /TASK>
     <TASK ID = "T4"> < /TASK>
   < /− Task definition− − >
   <!− Host Credential set definition− − >
     <HOST-CREDENTIAL ID = "H1",
          TYPE = "C1" / HOST-CREDENTIAL>
       <SUBJECT-PPROPERTY ID = "id11"
          OPERATOR = "op11" Value = "val11"
          PURPOSE-LEVEL = "level11">
       < /SUBJECT-PROPERTY>
       . . . . . .

       <SUBJECT-PPROPERTY ID = "id1n"
          OPERATOR = "op1n" Value = "val1n"
          PURPOSE-LEVEL = "level1n">
```

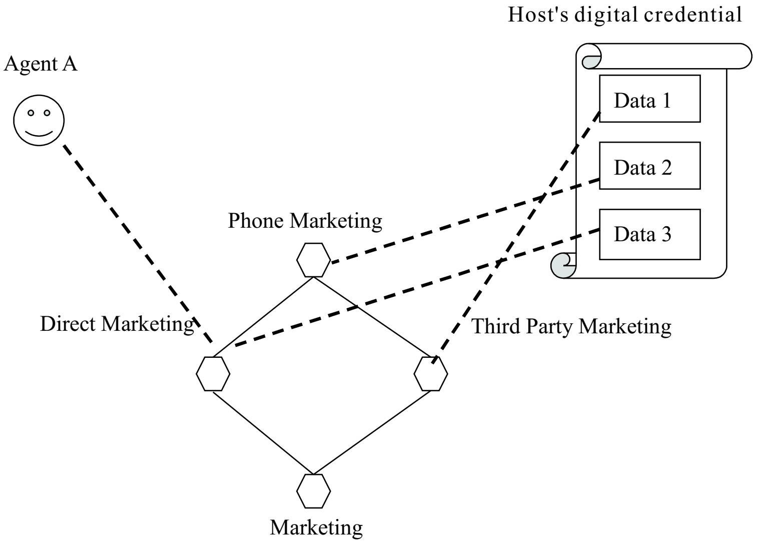

Figure 3: Purpose level of agent and host’s digital credential

```
        < /SUBJECT-PROPERTY>
      < /HOST-CREDENTIAL>
      <HOST-CREDENTIAL ID = “H2”,
          TYPE = “C2” / HOST-CREDENTIAL>
        <SUBJECT-PPROPERTY ID = “id12”
          OPERATOR = “op12” Value = “val12”
          PURPOSE-LEVEL = “level12”>
        < /SUBJECT-PROPERTY>
        ......

        <SUBJECT-PPROPERTY ID = “id2n”
          OPERATOR = “op2n” Value = “val2n”
          PURPOSE-LEVEL = “level2n”>
        < /SUBJECT-PROPERTY>
      < /HOST-CREDENTIAL>
    < / − − Host Credential set definition−− >

    <!−− Purpose of Host’s digital credential definition−− >
      <HOST-PURPOSE ID = “hp1”>
      < /HOST-PURPOSE>
      <HOST-PURPOSE ID = “hp2”>
      < /HOST-PURPOSE>
      <HOST-PURPOSE ID = “hp3”>
      < /HOST-PURPOSE>
      <HOST-PURPOSE ID = “hp4”>
      < /HOST-PURPOSE>
    < /−− Purpose of Host’s digital credential definition−− >
  < / − − Basic Elements −− >
  <! − − Relationships of Elements −− >
    <! − −Role hierarchy definition−− >
      <INHERITS FROM = “R1” To “R2”>
      < /INHERITS>
      <INHERITS FROM = “R1” To “R3”>
      < /INHERITS>
      <INHERITS FROM = “R2” To “R3”>
      < /INHERITS>
      <INHERITS FROM = “R2” To “R4”>
      < /INHERITS>
    < / − −Role hierarchy definition−− >
    <! − − Privilege assignment definition−− >
      <PRIVILEGE-ASSIGN TASK = “T1”
          PRIVILEGE = “O1”> < /PRIVILEGE-ASSIGN>
      <PRIVILEGE-ASSIGN TASK = “T2”
          PRIVILEGE = “O3”> < /PRIVILEGE-ASSIGN>
      <PRIVILEGE-ASSIGN TASK = “T3”
          PRIVILEGE = “O4”> < /PRIVILEGE-ASSIGN>
      <PRIVILEGE-ASSIGN TASK = “T4”
          PRIVILEGE = “O2”> < /PRIVILEGE-ASSIGN>
    < / − − Privilege assignment definition−− >
    <!− Task assignment definition−− >
      <TASK-ASSIGN ROLE =“R1” TASK = “C1”>
      < /TASK-ASSIGN>
      <TASK-ASSIGN ROLE =“R2” TASK = “C1, C4” >
      < /TASK-ASSIGN>
      <TASK-ASSIGN ROLE =“R3” TASK = “T4”>
      < /TASK-ASSIGN>
    < /− Task assignment definition−− >
    <!− Credential assignment definition−− >
      <CREDENTIAL-ASSIGN ROLE =“R2”
          CREDENTIAL = “C1”>
      < /CREDENTIAL-ASSIGN>
      <CREDENTIAL-ASSIGN ROLE =“R4”
          CREDENTIAL = “C2, C3”>
      < /CREDENTIAL-ASSIGN>
      <CREDENTIAL-ASSIGN ROLE =“R3”
          CREDENTIAL = “C3”>
      < /CREDENTIAL-ASSIGN>
    < /− Credential assignment definition−− >
    <!− Purpose hierarchy assignment definition−− >
      <PURPOSE-INHERIT FROM = “P1” TO =“P2”>
      < /PURPOSE-INHERIT>
      <PURPOSE-INHERIT FROM = “P1” TO =“P3”>
      < /PURPOSE-INHERIT>
    < /– Purpose hierarchy assignment definition–– >
  < / – – Relationships of Elements –– >
< /ERBAC-MODEL TYPE = “PRIVACY_POLICY”>
```

### 3.2 XML-based Privacy Policy of Mobile Agents

The privacy policy of agent is similar with the privacy policy of host. The policy includes the following two parts: (1) <! – – Basic Elements –– > defines basic elements of the model for agent including agent credential and purpose of agents; (2) <! – – Relationships of Elements –– > defines the relationships between the agent credential and purpose hierarchy of agents, an example of the privacy policy for agent is shown as below.

**Example 2: XML-based ERBAC Privacy Policy of Agent**

```
<? xml version= “1.0” >
< ERBAC-MODEL TYPE = “PRIVACY_POLICY”>
  <! – –Basic Elements–– >
    <!Agent Credential set definition – >
      <AGENT-CREDENTIAL ID = “H1”,
          TYPE = “C1” / AGENT-CREDENTIAL >
       <SUBJECT-PPROPERTY ID = “id11”
          OPERATOR = “op11” Value = “val11”
          PURPOSE-LEVEL = “level11”>
       < /SUBJECT-PROPERTY>
       ......

       <SUBJECT-PPROPERTY ID = “id1n”
          OPERATOR = “op1n” Value = “val1n”
          PURPOSE-LEVEL = “level1n”>
       < /SUBJECT-PROPERTY>
     < /AGENTT-CREDENTIAL>
     <AGENT-CREDENTIAL ID = “H2”,
          TYPE = “C2” / AGENT-CREDENTIAL>
       <SUBJECT-PPROPERTY ID = “id21”
          OPERATOR = “op21” Value = “val21”
          PURPOSE-LEVEL = “level21”>
       < /SUBJECT-PROPERTY>
       ......

       <SUBJECT-PPROPERTY ID = “id2n”
          OPERATOR = “op2n” Value = “val2n”
          PURPOSE-LEVEL = “level2n”>
       < /SUBJECT-PROPERTY>
     < /AGENTT-CREDENTIAL>
    < / –Agent Credential set definition–– >
    <!––Purpose of Agent’s digital credential definition–– >
     <AGENT-PURPOSE ID = “p1”>
     < /AGENT-PURPOSE>
     <AGENT-PURPOSE ID = “p2”>
     < /AGENT-PURPOSE>
     <AGENT-PURPOSE ID = “p3”>
     < /AGENT-PURPOSE>
     <AGENT-PURPOSE ID = “p4”>
     < /AGENT-PURPOSE>
    < / – –Purpose of Agent’s digital credential
           definition–– >
  < / – – Basic Elements –– >
  <! – – Relationships of Elements –– >
    <!– Purpose hierarchy assignment definition–– >
      <PURPOSE-INHERIT FROM = “P1” TO = “P2”>
      < /PURPOSE-INHERIT>
      <PURPOSE-INHERIT FROM = “P1” TO = “P3”>
      < /PURPOSE-INHERIT>
    < /–Purpose hierarchy assignment definition–– >
  < / – – Relationships of Elements –– >
< /ERBAC-MODEL TYPE = “PRIVACY_POLICY”>
```

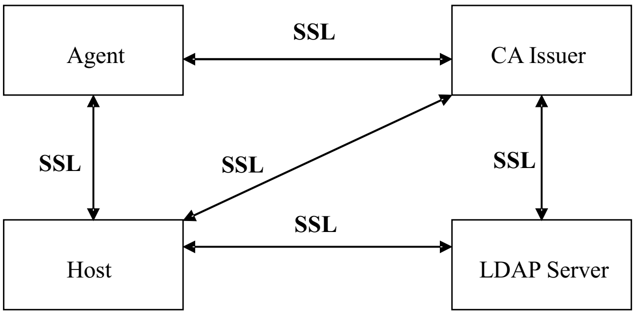

Figure 5: Management module of digital credentials

## 4 Architecture of the ERBAC Model

ERBAC deals with the security issues of Internet application by applying the proposed XML-based ERBAC security policy and a trust establishment strategy. The strategy is achieved by exchanging digital credentials between strangers in the Internet. When dealing with the privacy issues of digital credentials, the main problem is how to protect the privacy data of credentials when they are exchanged and transferred to strangers in the Internet environment. The core management element of the architecture is a privacy enforcement component.

### 4.1 Designing of a Privacy Enforcement Component

The privacy enforcement components are installed on mobile agents and hosts. Each mobile agent and host on the Internet has its own digital credentials that are gotten from CA issuers. In addition, hosts and agents have their XML-based privacy policies. Each time an agent is asked to submit its digital credential to host, the privacy enforcement component of the agent will be in charge of observing and protecting privacy data of the digital credentials according to agent’s privacy policy. Similarly,

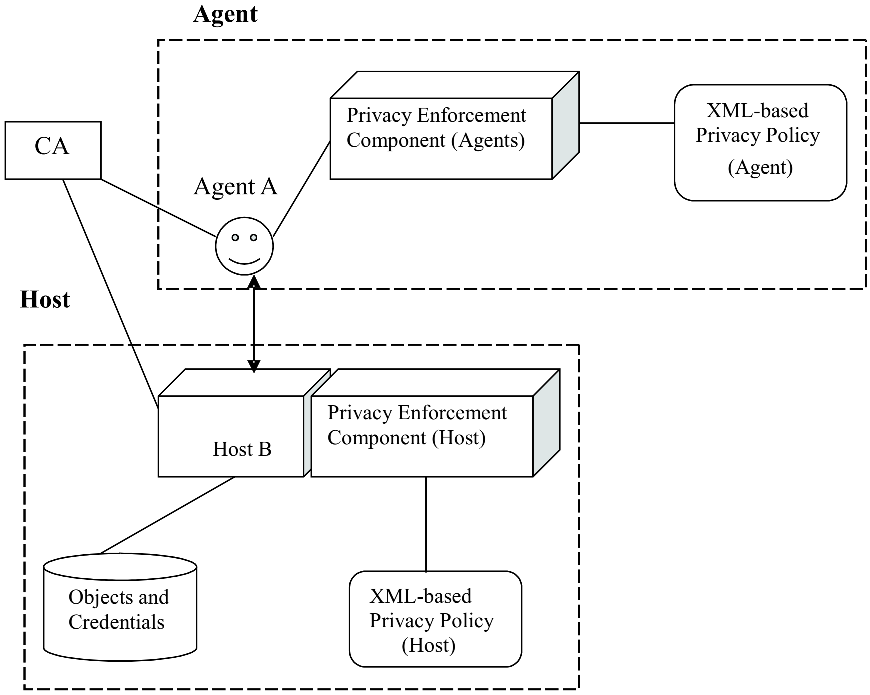
Agent
CA
Agent A
Privacy Enforcement Component (Agents)
XML-based Privacy Policy (Agent)
Host
Host B
Privacy Enforcement Component (Host)
Objects and Credentials
XML-based Privacy Policy (Host)

Figure 4: Architecture of ERBAC model

when a host is asked to submit its digital credentials to agent, the privacy enforcement component of the host will be in charge of observing and protecting privacy data of the host's digital credentials according to the host's privacy policy.

The general procedure of the architecture of the ERBAC model is shown in Figure 4 where we assume that agent A would like to apply for a role in host B in order to implement a task T on host B. If host B ask agent A to submit a credential for trust establishment according to XML-based privacy policy of the agent, the privacy enforcement component of the agent will check if the purpose level of host is higher or equal to the purpose level of the data in its credential. If yes, the credential will be sent to the host. Otherwise, the credential of the agent cannot be checked by the host. On the other hand, if the agent asks the host to provide its credential for trust establishment, the privacy enforcement component of the host will check if the purpose level of agent is higher or equal to the purpose level of the data in the credential of host according the XML-based privacy policy of the host. After the trust is established by exchanging credentials between agent and host, the privacy enforcement component of host parses its privacy policy and assigns a role to agent and furthermore assign the privileges to the agent to implement the required task.

## 4.2 Credential Management Component

A specially designed credential should associate itself with XML-based privacy policy. Also, it should be verifiable and unforgeable. Hosts or agents have the right to define and modify their XML-based privacy policy for their credentials. Moreover, using the Java and XML mobility, the rules of the privacy policy of the credentials could be loaded to mobile agents locally or from the network. The management component of the digital credential (Figure 5) is comprised of the agent, host, CA issuer and LDAP (Lightweight Directory Access Protocol) server. All information communicated among these components is encrypted by SSL protocol [13]. Assume that each element of the architecture has gotten an X509 V.3 public key certificate and a private key from a public key certificate facility [6, 7]. The main functions of each element of the architecture are described as follows:

- To access a privilege of a host, the agent applies for digital credentials from CA issuers.
- According to the ERBAC security policy, host requires and accepts certain kinds of digital credentials from the agent, assigns roles, and furthermore authorizes privileges to the agent.
- CA issuer is in charge of creating, issuing or revoking digital credentials for agents.
- LDAP server is the main component that is used to deal with the revocation problem of the digital credentials.

To deal with the authentication, revocation and privacy protection issues of the digital credentials, an authentication protocol, revocation protocol and an analysis of

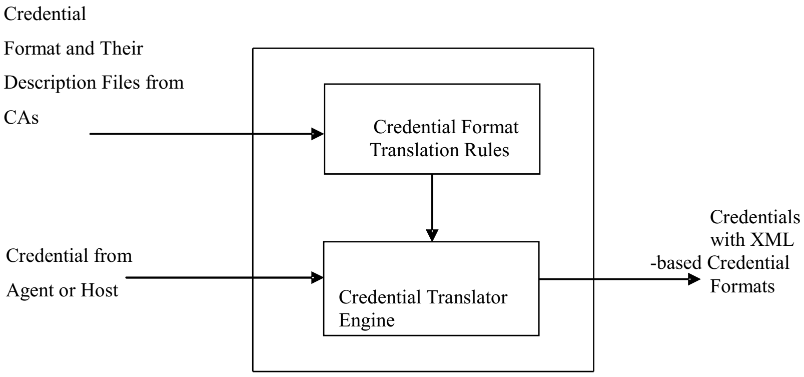
Credential Format and Their Description Files from CAs
Credential Format Translation Rules
Credential from Agent or Host
Credential Translator Engine
Credentials with XML -based Credential Formats

Figure 6: Credential translator module

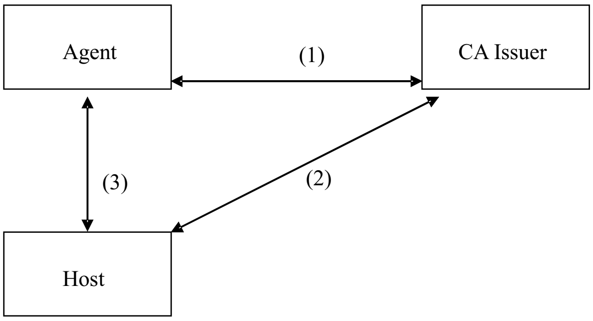

Figure 7: Authentication of digital credentials

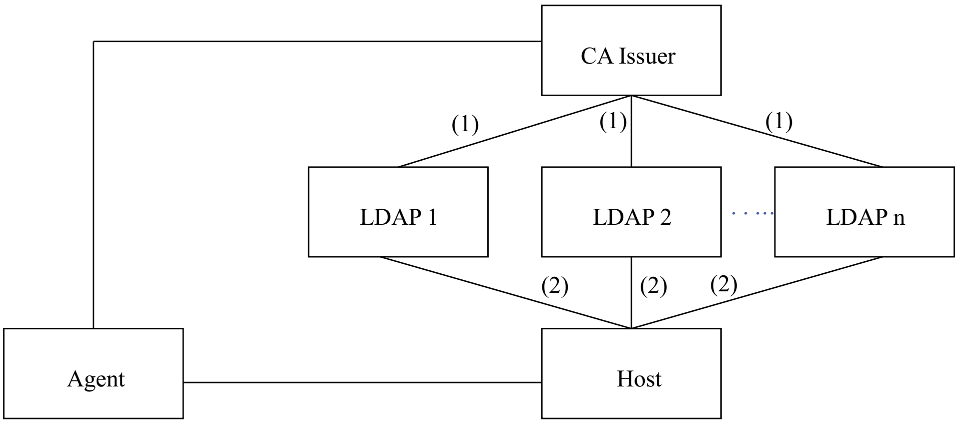

Figure 8: Credential revocation using LDAP

privacy protection are presented in the following Subsections 4.2.1, 4.2.2, and 4.2.3.

### 4.2.1 Authentication Protocol of Digital Credentials

The authentication protocol will be discussed among the following components: agent, CA issuer and host of the architecture (Figure 7).

1) Agent and CA Issuer
Establishing the connection between the mobile agent and CA issuer by SSL protocol and pre-configure the optional client authentication. The protocol is shown as follows:

    - The CA issuer authenticates the agent's X509 V3 public key certificate with the public key infrastructure and get the agent's public key from the certificate.
    - The agent applies for some kinds of digital credentials, for instance, driver's license, medical doctor credential, registered nurse credential, etc. from CA issuers. The agent provides the original paper documents of those credentials to the CA issuer.
    - After the paper credentials are approved, CA issuer gets the agent's public key from the agent's public key certificate and includes the public key in all the issued digital credentials for the agents.

2) CA issuer and Host
On normal conditions, we should handle credentials from multiple CAs, possibly even for the same credential type, the different CAs may use different credential formats. For instance, there are multiple formats for public key certificates ranging from different X.509 extension [12], to completely different credential formats such as PGP [11], SPKI [8], PolicyMaker [2] and KeyNote [5]. Therefore, a credential translator module is introduced and is shown in Figure 6. To handle a credential from multiple CAs, each credential type has its credential format and a description file defined by its CA issuer. The description file describes the format of the credential type. For any specific credential type, based on its credential formats and description document, credential format translation rules are introduced to convert the credential format to an XML-based credential format for the credential type (The format is defined in Appendix A). According to those rules, a credential translator engine is used to map credentials from agents or hosts into credentials with XML-based credential formats.

3) Agent and Host
Suppose mobile agent logs on the host and applies for a privilege and the host authenticate the agent as follows:
After establishing the SSL connection between the agent and the host, the host gets the public key of the agent from its public key certificate. The agent's public key certificate is authenticated by the SSL protocol.

    The host accepts the digital credential from the agent and authenticates it by comparing its public key of the credential with the agent's public key in its public key certificate. If they are equal, the digital credential will be authenticated. The authentication method between the agent and host is similar to the authentication method used in the SSL protocol. That is, if you trust a CA issuer, you should trust the digital credentials issued by the issuer.

### 4.2.2 Revocation Protocol of the Digital Credential

The revocation protocol of the architecture will be discussed among the agent, CA issuer, host and LDAP server from the architecture (Figure 8).

1) CA Issuer and LDAP Server
LDAP is the component dealing with the revocation problem of digital credentials. Whenever a credential is revoked, CA issuer sends a revocation proof to LDAP servers according to the locations of LDAP. The proof is comprised of a revocation message and its digital signature issued by the CA issuers. After accepting the revocation proof, the LDAP verify the proof and then store it to LDAP servers.

2) Host and LDAP server
Digital credentials issued by CA issuers contain the address of the LDAP server that has the revocation proof of the credential. Whenever an Internet user submits a digital credential to the host, the host always check the address of its corresponding LDAP server and make sure whether it has been revoked. If the digital credential is revoked, it will not be accepted.

### 4.2.3 The Analysis of Privacy Protection

Digital credential includes the public key of the agent and does not contain identity information of agents. Thus, a privacy protection method for digital credentials is provided. However, this solution makes it possible for the host to apply privileges from other hosts by using mobile agents' digital credentials. This problem has been solved because they don't have the private key of the user and cannot be authenticated. Moreover, under certain circumstances, the real identity of the agent is required to be presented and they could be disclosed directly from the CA issuers if approved.

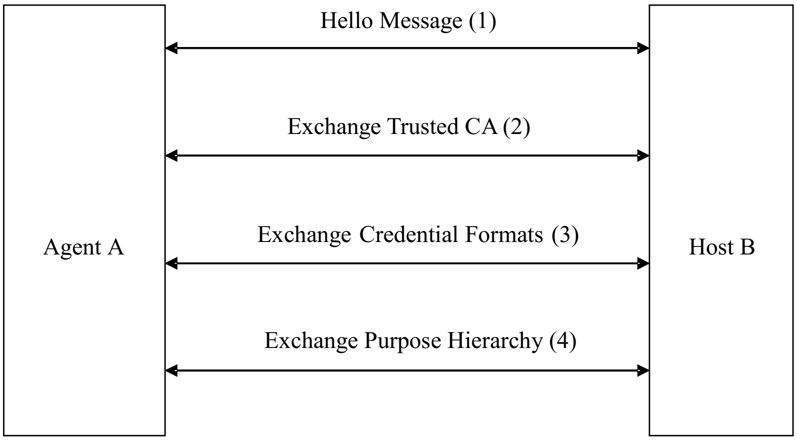
Hello Message (1)
Exchange Trusted CA (2)
Agent A
Exchange Credential Formats (3)
Host B
Exchange Purpose Hierarchy (4)

Figure 9: Protocol for communications between mobile agents and host

### 4.3 The Protocol for Communications between Mobile Agents and Host

The protocol between the mobile agent and hosts negotiates the privacy policy format that will be used, the purpose hierarchy and the credential CA and formats will be chosen. The system uses the same syntax of privacy policies and convertible XML-credentials.

The protocol (Figure 9) between hosts and agents of the architecture is shown as follows:

1) Agent A mobiles to Host B and sends a Hello message to B.

2) Host B and the agent A exchange their trusted CA and make sure the trusted CA should be existed in their trusted CA lists.

3) Host and mobile agent exchange their credential formats, the credentials and their formats on both sides should be the same or convertible.

4) Host and agent exchange the same purpose hierarchy and make sure the comparison of purpose levels of agent and host is built on the same purpose hierarchy.

## 5 Conclusion

In this paper, an Enhanced Role-based Access Control model (ERBAC) that addresses both security and privacy problems for Internet application is developed. Based on the mobile agents technique, an architecture of the ERBAC model is proposed and thus a system using mobile agents to automatically realize the authorization and privacy protection for Internet applications becomes feasible. The study, particularly the consideration and implementation of ERBAC model, will be used to provide valuable experience and good preparation to establish a more advanced role-based access control model and solve the security and privacy problems in the real Internet and mobile agent applications.

## References

[1] M. Blaze, J. Feignbaum, and J. Lacy, "Decentralized trust management," in *IEEE Symposium on Security and Privacy*, pp. 17–28, Oakland, CA, MAY 1996.

[2] M. Blaze, J. Feignbaum, and J. Lacy, "Decentralized trust management," in *IEEE Symposium on Security and Privacy*, pp. 17–28, Oakland, CA, MAY 1996.

[3] M. Blaze, J. Feignbaum, J, Ioannidis, and A. Keromytis, *Keromytis, The KeyNote Trust Management System*, ver. 2, Internet Draft RFC 2704, Sept. 1999.

[4] M. Blaze, J. Feignbaum, and A. D. Keromytis, "KeyNote: Trust management of public–key infrastructures," *6th International Workshop on Security Protocals*, pp. 59–63, Cambridge UK, 1998.

[5] M. Blaze, J. Feigenbaum, and A. D. Keromytis, "KeyNote: Trust management for public-key infrastructures," in *International Workshop on Security Protocols*, LNCS 1550, pp. 59–63, Springer-Verlag, 1998.

[6] D. W. Chadwick, " The ICE-TEL public key infrastructure and trust model," in *DIMACS Workshop on Trust Management*, New York, USA, 1996.

[7] D. W. Chadwick, "Deficiencies in LDAP when used to support a public key infrastructure," *Communications of the ACM*, vol. 46, no. 3, pp. 99–104, Mar. 2003.

[8] C. Ellison, B. Franz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen, *Simple Public Key Certificate*, Internet draft (expired), IETF SPKI Working Group, July 1999.

[9] J. Fan, K. Barker, B. Porter, and P. Clark, "Representing roles and purposes," in *Proceedings of the 2001 International Conference on Knowledge Capture (K-CAP'01)*, ACM, pp. 38–43, Oct. 2001.

[10] E. B. Fernandez, *An Overview of Internet Security*, http://www.cse.fau.edu/ ed/InternetSecOverview2.pdf.

[11] S. Garfinkel, *PGP: Pretty Good Privacy*, Sebastopol, CA: O'Reilly & Associates, Inc., 1995.

[12] R. Housley, W. Ford, W. Polk and D. Solo, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile,* RFC 2459, Draft Update draft-ietf-pkik-new-part1-06.txt, Jan. 1999.

[13] *OpenSSL: OpenSSL ver. 0.9.7*, http://www.openssl.org/, Dec. 31, 2002.

[14] C. S. Powers, P. Ashley, M. Schunter, and P. Promise, "Access control, and privacy management," in *Proceedings of the* $3^{rd}$ *International Symposium on Electronic Commerce*, IEEE, pp. 13–21, 2002.

[15] C. Ribeiro, A. Zuquete, P. Ferreira, and P. Guedes, "SPL: An access control language for security policies with complex constraints," in *Network and Distributed System Security Symposium (NDSS01)*, San Diego, California, 2001.

[16] R. S. Sadhu, "Role-based access control models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, Feb. 1998.

[17] K. Seamons, M. Winslett, T. Yu, L. Yu and R. arvis, "Protecting privacy during on-line trust negotiation," in *Proceedings of Workshop on Privacy Enhancing Technologies (PET)*, pp. 129–143, San Francisco, Apr. 2002.

[18] M. P. Gallaher, A. C. o'Connor, and B. Kropp, *The economic impact of role based access control*, Research Triangle Institute, NIST Planning Report, 02-01, 2002.

[19] M. Winslett, T. Yu, K. E. Seamons, A. Hess, J. Jacobson, R. Jarvis, B. Smith, and L. Yu, "Negotiatingtrust on the Web," *IEEE Internet Computing*, vol. 6, no. 6, pp. 30–37, Nov. 2002.

[20] C. Yang and C. N. Zhang, "Secure Web-based applications with XML and RBAC," in *4th Annual IEEE Information Assurance Workshop*, United States Military Academy West Point, New York, June 2003

[21] C. Yang and C. N. Zhang, "Designing secure E-Commerce with role-based access control," in *IEEE Conference on E-Commerce (CEC'03)*, pp. 313–319, Newport Beach, California, USA, June 2003.

[22] T. Yu, M. Winslett, and K. E. Seamons, "Supporting structured credentials and sensitive policies through interoperable strategies in automated trust negotiation," *ACM Transactions on Information and System Security*, vol. 6, no. 1, pp 1–42, Feb. 2003.

# Appendix A

**Specifications of XML-based Credential Format:**

ERBAC defines an $XML - basedcredential$ format for each credential type and the syntax of credential defines an XML tag CREDENTIAL, an attribute ID which value is $credential - id$ and an attribute TYPE which value is $credential - type$.

```
<! –Credential definition– >
< CREDENTIAL ID = credential-id,
            TYPE = credential-type>
< SUBJECT-PPROPERTY ID = property-id(1)
            OPERATOR = subject-operator(1)
            Value = property-value(1)>
< /SUBJECT-PROPERTY>
    ......
< SUBJECT-PPROPERTY ID = property-id(n)
            OPERATOR = subject-operator(n)
            Value = property-value(n)>
< /SUBJECT-PROPERTY>
< /CREDENTIAL>
```

We assume there are n subject properties and the subject properties in the credential type. The syntax of subject property defines an XML tag SUBJECT-PPROPERTY, an attribute ID which value is $property - id$, an OPERATOR attribute which value is $subject - operator$, such as " > " " < " " = ", etc, and an attribute Value which is $property - value$.

**Cungang Yang** received the M.S degree in computer science from Jilin University, China. He completed his Ph.D degree in computer science in 2003 at University of Regina, Canada. In 2003, he joined the Ryerson University as an assistant professor in the Department of Electrical and Computer Engineering. His research areas include security and privacy, enhanced role-based access control model, information flow control, web security and secure wireless sensor networks.