Abstract

In this paper, four security frameworks in agent-based systems, 1) a policy based approach to security for the agent-based Semantic Web; 2) a privilege management scheme for mobile agent systems; 3) a two-layer architecture with security layer on top of FIPA-OS; and 4) an adapted role based access control for MARISM-A using SPKI Certificates; are assessed by using the selected criteria of security, flexibility and expandability, distributed policy management, and speech acts. The result of this evaluation shows that a policy based security framework [10] provides the most potential security framework for the agent-based Semantic Web.

1 Introduction

Berners-Lee [1] envisions the Semantic Web to be a web that can understand and interpret web pages and manage activities for people. The Semantic Web will bring structure to the meaningful content of Web pages, creating an environment where software agents can readily carry out sophisticated tasks for users.

With the development of Web technologies (Web Services, XML, RDF, DAML+OIL, web agents and ontologies) [6], the agent-based Semantic Web makes use of the full capabilities of the existing infrastructure and information available on the Internet, and integrates multi-agent systems with the Web. Security is a fundamental concern for a mobile agent system [3, 4, 7]. New security risks related to the agent-based Semantic Web have emerged [2] with the development of applications built on these web technologies. These security threats include authentication, authorization, auditing, data privacy, data integrity, availability, and non-repudiation [11]. One of the major concerns is the security threat to the agents and agent platforms which can be classified as 1) agents attacking platforms; 2) agent platforms attacking agents; 3) agents attacking agents [9].

There are many security techniques that may be applied in agent-based systems [8], such as: 1) Isolation of agents from the computational environment and from one another; 2) Language and code safety; 3) Controlled access to and limited consumption of resources; 4) Audit by both agents and platforms; 5) Authenticated and protected communications; 6) Signed code; and 7) Partial result encapsulation.

In this paper, a simple model of an agent-based system is assumed with two main components: agents and the agent platforms. An agent is a software program, either an independent process or a lightweight thread, which executes autonomously and carries out some specified task in a computational environment on behalf of a user. The agent platform provides such a computational environment, involving a single host computer or multiple hosts, in which an agent can be instantiated, interact with other agents, and use platform services for all registered agents.

The remainder of this paper is organized as follows: Section 2 contains a brief overview of the four security frameworks in the agent-based systems to be assessed. Section 3 provides the description of the selected criteria for the assessment of the security frameworks in this paper. The selected criteria are applied to each of the security frameworks and the results are summarized in a table format for easy review. The results and some discussion are presented in Section 4 and the conclusion and future work is in Section 5.

2 Overview of the Four Security Frameworks in Agent-Based Systems

There are many different kinds of architectures used to support agent-based systems, but all implementations should include a security framework to provide countermeasures against the common security threats to the agents and agent platforms described in Section 1. Four security frameworks have been selected for assessment from the most recently developed and commonly used frameworks. The selected frameworks are; 1) a policy based approach to Security for the agent-based Semantic Web [10]; 2) a privilege management scheme for mobile agent systems [8]; 3) a two-layer architecture with security layer on top of FIPA-OS [13]; and 4) an adapted role based access control for MARISM-A using SPKI Certificate [12]. Each of the four security frameworks is described briefly below.

2.1 A Policy Based Approach to Security for the Semantic Web

Kagal et al [10] present a policy based security framework for the agent-based Semantic Web and propose a distributed policy management approach that uses a semantic policy language to define security requirements for web entities in the agent-based Semantic Web. The policy language and distributed policy management could be uniformly applied to web entities such as web resources, agents and web services.

According to [10], a policy includes a set of rules that associate a required set of credentials with certain ability or right for an individual, group or role based web entity. The framework uses an external authentication process,
such as Public Key Infrastructure (PKI), to verify credentials in order to grant permission for the associated action. The policy language provides a flexible structure to specify a policy in terms of properties of web entities including their identities, actions, speech acts and permissions, prohibitions, obligations, and dispensations. With distributed policy management, it is possible for each web entity to specify or enforce its own policies.

The agent-based system described in the paper [10] follows the Foundation for Intelligent Physical Agent (FIPA) specifications [5]. The Agent Management System (AMS) maintains a directory of registered agents and provides a white page service of the registered agents in the agent platform. The Directory Facilitator (DF) provides a yellow page service of all the services offered by the registered agents, and the agent platform is available to other agents. Security enforcement is required to protect the agents and agent platforms against the common security threats in the following four actions: 1) agents registering with AMS; 2) agents querying the AMS; 3) agents registering their services with the DF; and 4) agents querying the DF for services offered by registered agents. An agent sends policies containing its service, access control information, category, etc., to the DF and/or the AMS while registering with the AMS so that the AMS or DF can decide whether to provide the service to other requesting agents by checking these policies. The agent platform checks the distributed policies to decide whether to allow an agent to register with the AMS or the DF. An agent could delegate permissions to the set of agents according to its own policy.

### 2.2 A Privilege Management Scheme for Mobile Agent Systems

Jansen [8] presents a privilege management scheme where security rules related to agents and the agent platform are embedded in an attribute certificate bound to an agent or a policy certificate bound to the agent platform. The security policies are prescribed in external XML files and stored in the agent platform. The policy engine uses an attribute certificate to validate the certificate and enforces security policies on the agent to control the resource access rights, and uses the policy certificate to enforce security policies on the agent platform to control the behavior and access rights of all agents visiting the agent platform. The security rules of the attribute certificate could be adjusted in order to meet the various security requirements for the particular agent by the policy-setting principal which could be any entity issuing privilege management certificates.

According to Jansen [8], there are three kinds of policy-setting principals, a hosting principal, a branding principal and a use principal. A hosting principal controls the resource authorization over the agent platforms and issues the policy certificate. A branding principal or a use principal controls the resource authorization over the agents and issues attribute certificates.

The privilege management scheme [8] also allows privilege authorization and delegation from a policy-setting principal to others through the use of a privilege management certificate following the functionality and security requirements, and the policies.

### 2.3 Two-Layer Architecture with Security Layer on Top of FIPA-OS

Zhang [13] proposes a two-layer architecture with a security layer on top of FIPA-OS, as shown in Figure 1. The FIPA-compliant agent platform (FIPA-OS) is responsible for agent management and communication, and the security layer provides three security-related services, authentication and authorization, a secure communication and a secure execution environment. As the two major components of the security layer, the Secure Agent Channel Communication (SACC) and the Credential Granting Center (CGC) are also the agents registered in the Agent Management System (AMS). There are two types of authentication processes implemented in the security framework - platform authentication and agent authentication. In order for the platform to provide secure communication, the platform mutual authentication process is performed by exchanging and verifying platforms’ certificates, which contain platforms’ names and public keys of Public Key Infrastructure (PKI). The Credential Granting Center (CGC) in the security layer of the agent platform performs agent authentication to verify the identity of an agent and its owner. A permission credential consisting of attributes associated with the agent’s identity and its associated access rights in the platform will be issued to the agent by CGC after the Policy Server (PS) decides what authorizations should be granted to the agent based on the pre-defined policy criteria. The integrity and authenticity of a valid permission credential is guaranteed by PKI and encryption of the whole credential permission. Since it regards the communication between agents as the interactions of different communicative acts, a FIPA-compliant agent platform uses agent communication language (ACL) to send encoded text messages. It becomes necessary to protect the data integrity and confidentiality during transmission; therefore, the secure communication channel in the security layer of the security framework is established to meet this security requirement by using cryptography technologies.

The secure execution environment service provided by the security layer of the security framework enforces the security protection of platform resources and agent services, and only agents with valid permission credentials can access these resources and services.

### 2.4 Adapted Role-based Access Control for MARISM-A using SPKI Certificates

Navarro et al [12] present a security framework layered on the top of FIPA OS. This security framework consists of four major components: authorization manager (AM), role manager (RM), certificate repository manager (CRM), and resource manager (DM). The main features of the role-based access control method and trust management for the mobile agent systems are the role system and the delegation of authorization to the mobile agents by using Simple Public Key Infrastructure (SPKI). For example, if a principal globally identified by its public key is authorized to access a resource as a role member, it automatically has all the authorizations specified for that role.
The main functionality of the resource manager (DM) is to control the resource access and verify the resource access request with the master SPKI key. The main functionality of the authorization manager (AM) is to manage the delegation of authorizations and issue authorization certificates to roles following its local authorization policy. The purpose of the role manager (RM) is to assign and manage the role definition and membership by issuing SPKI name certificates. The certificate repository manager (CRM) is responsible for implementing and managing a certificate repository that provides certificate query services.

3 Evaluation of the Security Frameworks in Agent-Based Semantic Web

In order to assess the four security frameworks against the same standard, the following criteria are considered as the important characteristics for a security framework in an agent-based system and are used as the basis for the evaluation process.

3.1 Criteria and Metrics

The following four criteria have been chosen to carry out the assessment of the four security frameworks described in Section 2. These criteria are considered most important for capturing qualities in the security framework because they address the key aspects important to its success. The criteria are measured by ordinal measurement and are associated with metric values of good, fair, poor. The default of poor value will be used if a security framework does not define a stakeholder. These criteria and metrics are defined for each criterion below:

Security: Security is the basic criteria for a security framework. For agents and agent platforms, some countermeasures against the security threats should be implemented to protect agents against the outside network and to protect platforms against unauthorized access. The common security countermeasures related to the security framework of the agent-based system should include: 1) authentication mechanism to allow the mutual authentication of agent platforms and agents to verify their identities; 2) authorization to allow agents to access the platform resources; 3) data integrity and confidentiality during transmission. A framework is considered good if the framework provides a secure execution environment for both the agent and the agent platform, and the system should be impervious to common security threats described above. A framework is considered fair if the framework addresses some security issues and poor if the framework fails to provide countermeasures against the common security threats.

Flexibility and expandability: The flexibility and expandability of the framework requires a separate security architectural layer that provides security protection across various services to achieve independence of the security mechanisms. A framework is considered good if the framework has a separate security layer to provide security related services to agents and agent platforms with a bypass option if necessary. A framework is considered fair if it provides a separate security layer but without the option to bypass security. A framework will be considered poor if it does not use a separate architectural layer and embeds security policies and decision points into the application.

Figure 1. The Two-Layer Structure with a Security Layer on Top of FIPA_OS [13]
Distributed policy management: The widely distributed, decentralized and open applications found in the agent-based Semantic Web require distributed policy management and the uniform application of the security policies to all the web entities (web pages, agents, human users and web services), which access resource or interact with a given web entity. A framework is considered good if the framework uses a distributed policy management and the security policies are uniformly applied to all web entities. A framework is considered fair if the framework uses a distributed policy management but fails to apply the security policies uniformly to all web entities. A framework is considered poor if the framework uses a form of centralized policy management and control.

Speech Acts: The speech acts allow web entities to update existing policies automatically, such as the delegation of permissions, the revocation of the permissions, and the cancellation of previous requests. Delegations are important to an agent-based system because the security requirements of web entities cannot be determined in advance, and the specific web entity that will access the web resource may not be known. A framework is considered good if it provides all these capabilities, a framework is considered fair if the framework supports some of them, and a framework is considered poor if the framework does not support any of these capabilities.

3.2 Methodology

The four security frameworks of the agent-based systems described in Section 2 were reviewed, and each security framework was assessed against the selected criteria described in Section 3.1. An ordinal measurement of poor, fair and good was given to each criterion for each framework. In order to calculate the overall score of each security framework, the ordinal measurement of good, fair and poor was mapped into the numerical values of 2, 1 and 0, respectively. The overall score of the security framework was defined as the sum of all numerical scores of the criteria of the security framework. The higher the overall score, the better the framework should be. The best security framework is the one with the highest overall score in terms of the selected criteria described in Section 3.1.

4 Results

Each of the four security frameworks has been assessed against the selected criteria described in Section 3.1 and the results are summarized in Table 1. The overall score of the security framework was calculated and the policy based security framework [10] received the highest score of 1.25, and a privilege management scheme for mobile agent systems [8] is given the lowest score of 0.75. The two remaining approaches fell in between with a score of 1.00.

From the point view of security, all of the four frameworks provide some form of authentication and authorization mechanisms, such as PKI etc. Adapted role-based access control [12] uses the relations between users – roles, and permissions – roles and local role policy to authenticate and authorize the web entities by granting SPKI authorization certificates and name certificates which are used by the Resource Manager to control the access to a resource and delegate authorizations to the Authorization Manager. The policy based security framework [10] computes the access rights not only from the users’ role, but also based on the different credentials and properties of entities associated with the users. The policy based security framework [10] uses external authentication and authorization mechanisms for verifying credentials, such as SPKI. A Privilege Management Scheme for Mobile Agent Systems [8] provides authentication and authorization mechanisms by issuing two kinds of certificates, the attribute certificate and the policy certificate, based on the externally prescribed security policy in XML files. In the two-layer architecture with security layer on top of FIPA-OS [13], the Certificate Authority (CA) is issued to an agent and an agent platform respectively after the authentication by the Credential Granting Center according to the policy file, and is treated as the root of the trust.

FIPA-compliant agent platforms do not fully address potential security threats to agents and agent platforms such as data integrity and confidentiality, integrity of transactions and communications. FIPA-compliant agent platforms treat the communication between agents as the interactions of different communicative acts and are carried out via the sending of encoded text messages using Agent Communication Language (ACL). Therefore, it is important to establish a secure communication channel between two FIPA agent platforms to prevent most common third party threats. The security layer of the two-layer architecture with security layer on top of FIPA-OS [13] provides such a secure communication channel and protects data integrity and confidentiality by using cryptography technologies. Adapted role-based access control for MARISM-A using SPKI Certificates [12] addresses this issue by using Secure Sockets Layer (SSL) to provide both confidentiality and authentication for agency communication.

The assessment of fair for the criteria of security is given to the policy based security framework [10] and a privilege management scheme for mobile agent systems [8] since both of them do not explicitly address countermeasures to assure data integrity and confidentiality.

The benefit of the separation of the security architectural layer is independence of the security mechanisms. The separation of the security layer from the agent platform makes it possible to provide all security related services inside the security layer, and to decouple security mechanisms and policies from specific agent platforms. Therefore, it is possible to provide the needed protections across various services in a dynamic and flexible fashion and realize the independence of the security mechanisms. Among the four security frameworks assessed, the two-layer architecture with security layer on top of FIPA-OS [13] and adapted role-based access control for MARISM-A using SPKI Certificates [12] provide the separate modular security layer, but the former has the freedom to bypass the security layer if necessary.
Table 1. Results of the assessment of the four security frameworks

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Security</th>
<th>Flexibility &amp; Expandability</th>
<th>Distributed Policy Management</th>
<th>Speech Acts</th>
<th>Overall Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy based Security Framework [10]</td>
<td>Fair</td>
<td>Poor</td>
<td>Good</td>
<td>Good</td>
<td>1.00</td>
</tr>
<tr>
<td>A Privilege Management Scheme for Mobile Agent Systems [8]</td>
<td>Fair</td>
<td>Fair</td>
<td>Poor</td>
<td>Fair</td>
<td>0.75</td>
</tr>
<tr>
<td>Two-Layer Architecture with Security Layer on Top of FIPA-OS [13]</td>
<td>Good</td>
<td>Good</td>
<td>Poor</td>
<td>Poor</td>
<td>1.00</td>
</tr>
<tr>
<td>Adapted Role-based Access Control for MARISM-A using SPKI Certificates [12]</td>
<td>Good</td>
<td>Fair</td>
<td>Poor</td>
<td>Fair</td>
<td>1.00</td>
</tr>
</tbody>
</table>

There are many different web entities (web pages, agents, human users and web services, etc.), which access web resources or interact with other web entities in the distributed, decentralized and open systems in the agent-based Semantic Web. It will be beneficial for each individual web entity to be able to make its own security requirements decisions and, on the other hand, to have the security policies applied uniformly to all kind of web entities. All security frameworks, except the policy based security framework [10], use a centralized approach to policies management and control. These centralized approaches are specified by single set of individuals, about a predetermined set of users and resources and have a single location with a central point of control [10]. The policy based security framework [10] not only supports the distributed policy management, but also supports the application of security policies uniformly to all web entities like web services, agents, and human users in the agent-based Semantic Web.

Support of speech acts, especially delegations, is important to the inherently distributed agent-based Semantic Web since the security requirements of the web entities cannot be determined in advance, and it is unknown which web entity will access the web resource. The ability to delegate makes it possible to propagate and dynamically change the access rights of a web entity without explicitly changing its policy or security requirements. Among the four security frameworks assessed, only the two-layer architecture with security layer on top of FIPA-OS [13] does not support speech acts, such as the delegation of permissions, the revocation of the permissions, and the cancellation of the previous requests. The policy based security framework [10] fully supports Speech Acts.

5 Conclusion and Future Work

In this paper, we have assessed four security frameworks used in agent-based systems and have identified the potentially most secure framework for use on the agent-based Semantic Web. We have selected the criteria of security, flexibility and expandability, distributed policy management, and speech acts as the group of important characteristics for such a security framework. We have evaluated each of the four security frameworks by using the selected criteria with the ordinal measurement of poor, fair and good and results are summarized in Table 1.

Our work shows that policy based security framework [10] has the highest overall score and provides the most potentially secure framework for the agent-based Semantic Web. Note that a score of fair was given to the flexibility and expandability criterion since the security framework does not use a separate security layer to provide the security service and flexibility to protect agents and agent platforms. The score of fair was also given to the security criterion since the security framework does not provide or address explicitly the secure communication channel to secure data integrity and confidentiality during transmission. The two-layer architecture with security layer on top of FIPA-OS [13] provides these two features missing in the policy based security framework. For the future work, an ideal security framework would result if two security frameworks, the policy based security framework and the two-layer architecture with security layer on top of FIPA-OS, could be combined together. That is, if the policy based security framework could implement the concept of the two-layer architecture with security layer on top of FIPA-OS, or use a separate security layer to provide the security service and flexibility to protect the agents and agent platforms.

References