

A Privacy Component and Universal Privacy Ontology for FIPA Agent Platforms

Regina M. Mathis
Nova Southeastern University
mregina@nova.edu

Abstract

While there is much research and development activity taking place regarding the Semantic Web, privacy is an important issue that is often overlooked. In order for the Semantic Web to become acceptable to modern society, privacy rights must be addressed. This research project will address the privacy issue by first building a Privacy Component into the foundation of agent communication, and second, creating a Universal Privacy Ontology.

The first phase of the project is to represent the framework for the Privacy Component. The Privacy Component will be incorporated into the two-layer architecture presented in Zhang, Karmouch, and Impey [5], which is proposed to add security features as the security extension to the FIPA specification. The second phase of the project is to define a Universal Privacy Ontology that will be used to create privacy policies that are both customizable and flexible.

1. Introduction

The next generation World Wide Web is quickly approaching. Once in fruition, the Semantic Web will change our lives dramatically. One day in the very near future, machines will be able to locate, organize, and integrate available information. Machines, called agents will be able to plan events and daily activities for humans.

Enabling machines to understand data is a very powerful capability. Because agents will plan and manage all aspects of life on a daily basis, the agents will have access to all types of personal information. Agents could exchange personal information about a user, compile databases about online preferences and habits, including sites visited, items purchased, interests, and hobbies and so on. The potential assault on privacy rights is a major deterrent for the proliferation of the Semantic Web [4].

Privacy issues are often overlooked and have not been built into the foundation of the Semantic Web. Privacy and security are major concerns because the Semantic Web is both decentralized and diverse. It is extremely difficult to implement a set of generic policies that apply to all users. The Platform for Privacy Preferences (P3P) specification, which is used in the Web of today, describes privacy policies using XML to display policies in a standardized machine-readable format [4]. P3P uses a baseline set of data elements which can be used to describe the type of data that is frequently collected from Web sites and it is then referenced in the sites' privacy policies. The problem with P3P being used in the Semantic Web is that it allows sites to declare additional data elements to be captured by publishing their own schemas. On the Semantic Web, agents will capture and compile information to suit a user's needs and in order for agents to be able to compare service providers, understanding this additional information and how it is to be used is a major concern [4].

Consider the case where you want to buy a house. Your agent queries the agents of different lending institutions for interest rates according to your specifications and credit rating. Your agent finds the best rate and applies for the mortgage. Before the final approval is granted, you must provide proof of a homeowner's insurance policy. Your agent queries the agents of

insurance companies over the internet and finds three suitable insurance companies. It then applies for a policy with the company with the best insurance rating and shortest turnaround time. Your agent provides the mortgage agent with the policy information. The mortgage agent contacts the insurance agent requesting proof of insurance. The insurance agent confirms that you have valid insurance in a digitally signed message. There are three parties involved that must form a trusted relationship.

This scenario involves privacy protection, trust and security. First, all three parties need to form a trusted relationship. Within this relationship, security protocols need to be established to protect the confidentiality of the purchaser's financial information. Privacy protocols also need to be established to protect the same confidentiality as well as to ensure that the insurance agent does not know the social security number and financial details of the purchaser. It would be necessary to ensure that the insurance agent only knows the purchaser, property location, purchase price, mortgager, and mortgage amount.

Using the P3P specification, lending institutions could create their own schemas to define data elements [4]. One mortgage agent may call it interest rate, another may call it APR and still another may call it annual rate. If the purchaser's agent was on the Semantic Web comparing mortgage agents for their privacy policies, and the mortgage agents created their own data elements to describe their privacy policies regarding mortgage interest rates, the agent would not be able to compare the privacy policies received from the different mortgage agents.

A Universal Privacy Ontology would remedy part of this problem. The multiple interaction between agents in the Semantic Web will require that agents communicate with one another using an agreed upon process to protect the privacy of their respective users [4]. In this ontology, data elements would be defined with parameters and index terms to eliminate any potential for misunderstanding. The schema could be extended for special data elements but the core data elements would be uniform across all agents.

The Foundation for Intelligent Physical Agents facilitates interoperability among different agent platforms. Any agents that are FIPA compliant, regardless of the type of system and provider used, can communicate and interact with each other using Agent Communication Language (ACL).

Privacy, along with security, are issues that have yet to be addressed in the latest version of the FIPA specification. In the FIPA2002 Agent Message Transport Service Specification Standard, the FIPA2002 Agent Management Specification Standard, and the FIPA2001 Ontology Service Specification Experimental, there is no mention of a privacy specification. The FIPA2002 Abstract Architecture Specification Standard discusses content privacy in terms of encrypting software, a message or other data, and sending over a secure communication channel. There are no provisions of any type for behavioral privacy policies or components.

The reason why privacy is omitted from the FIPA specifications is due to the fundamental purpose of the FIPA specification. FIPA allows different agent platforms to interact and communicate with one another. Because of this, FIPA defines only the abstract architecture and logical components of each agent platform [5].

In order to include privacy in the abstract architecture, there needs to be a privacy abstraction for the different models of concrete implementation. Because [5] have provided a security abstraction, which include secure communication channels; the Privacy Component will be added to the security abstraction.

It is important to mention that the privacy design cannot be completely contained in the Privacy Component. Privacy must be a part of the software infrastructure, into which the agent

platform is embedded. For this reason, agents will interact with both a Privacy Component and the Universal Privacy Ontology.

2. Project Summary

Privacy is a concern for most users of the Internet and this trend will continue with the proliferation of the Semantic Web. To address this concern, this research project will address the privacy issue by first building a Privacy Component into the foundation of agent communication, and second, creating a Universal Privacy Ontology. The project has two phases of development.

The first phase of the project is to represent the framework for the Privacy Component. The Privacy Component will be incorporated into the two-layer architecture presented in [5], which is proposed to add security features as the security extension to the FIPA specification. The Privacy Component is the mechanism and will contain a basic set of data elements for all users. The second phase of the project is to define a Universal Privacy Ontology that will be used to create privacy policies and can be customized to allow additional data elements to be defined. The Universal Privacy Ontology will clearly define various types of privacy, for example, privacy of personal behavior versus privacy of communication channels [4].

The Universal Privacy Ontology is used to create the privacy policy and is separated from the Privacy Component for flexibility. Policies will change but the underlying mechanism need not change, merely withstand minor updates.

The intellectual merit of this research project lies in the ability to further advance technological growth in the areas of semantic search and retrieval tools, agent technology, and ontological development tools all within a framework that incorporates privacy into its foundation. The proposed project suggests an organized and innovative approach to the inclusion of privacy considerations and rights into agent interoperability and communication so that the Semantic Web can be utilized to its full potential, safely, securely and respectably.

3. Project Description

The first phase of the project is to represent the framework for the Privacy Component. The second phase of the project is to define a standardized privacy ontology which can be customized to allow additional data elements to be defined.

3.1. Phase One Development – Privacy Component

Phase one of the project is to develop the Privacy Component for the two-layer architecture presented by [5], which is proposed to add security features as the security extension to the FIPA specification. FIPA agent standards support several agent platforms including FIPA-Open Source (FIPA-OS), JADE, Grasshopper and ZEUS [5]. The agent platform used in the two-layer architecture is FIPA-OS and is implemented using Java. The two-layers are 1) a secure communication service which prevents any eavesdropping or tampering from the outside network and 2) a secure execution environment service, which protects server resources from unauthorized access [5]. This security extension does not provide a mechanism to administer or control privacy policies.

3.1.1. Overview of Two-layer Architecture. There are three major mechanisms in the Two-layer Architecture. The first is Authentication. Authentication mechanism handles the process of allowing legitimate system entities to process tasks while denying illegitimate ones. This mechanism includes platform authentication and agent authentication.

The second is Secure Communication, which ensures a secure communication channel between two FIPA agent platforms. FIPA defines communication as communicative acts between a sender and receiver using formal Agent Communication Language (ACL) [1]. In FIPA, ACL is a standard communication language that defines the encoding Semantics and the specifics of the messages. Agents are able to activate the secure communication service of its current platform by inserting security parameters into an ACL message [5].

The third mechanism is Resource Monitoring, which serves to protect some platform resources and agent services from unrestrained access. Resource monitoring also ensures that only authorized agents are given access to these resources and services.

3.1.2. Layer Dynamics. The underlying layer is the FIPA-OS agent platform layer. This layer is responsible for agent management and the communication infrastructure. It includes mandatory elements contained in the FIPA97 specification and also supports agent interoperability [5].

The Security layer is the upper layer and is a security extension to FIPA-OS. This layer provides security-related services to agents and it relies greatly on the underlying agent platform for communication and agent management. Currently it contains the Secure Agent Communication Channel (SACC), which provides a secure channel for agent communication, in part by requesting service provided by the Agent Communication Channels (ACC) in the FIPA-OS, and the Credential Granting Center (CGC). Both of these are agents registered in the Agent Management System (AMS) of the local FIPA-OS agent platform [5].

Privacy requires trust and security along with a standard method of exchanging privacy policies. The Privacy Component (PC) is to be the newest component of the Security Layer. The reasons for separating the Security Layer from the FIPA-OS Layer are that it frees the security mechanisms and policies, and thus the privacy mechanisms, from specific agent platforms. In addition, only services defined in the FIPA specification are used by components in the security layer. This ensures that the Privacy Component will only involve the defined functions of the underlying agent platform rather than the details of its implementation. Figure 1 shows the two-layer architecture.

The principal benefits of this approach are that the Privacy Component is independent and that different platforms with specific security mechanisms are able to interact under the same security architecture and the Privacy Component is transparent to all platforms. This architecture complies with the goal of FIPA.

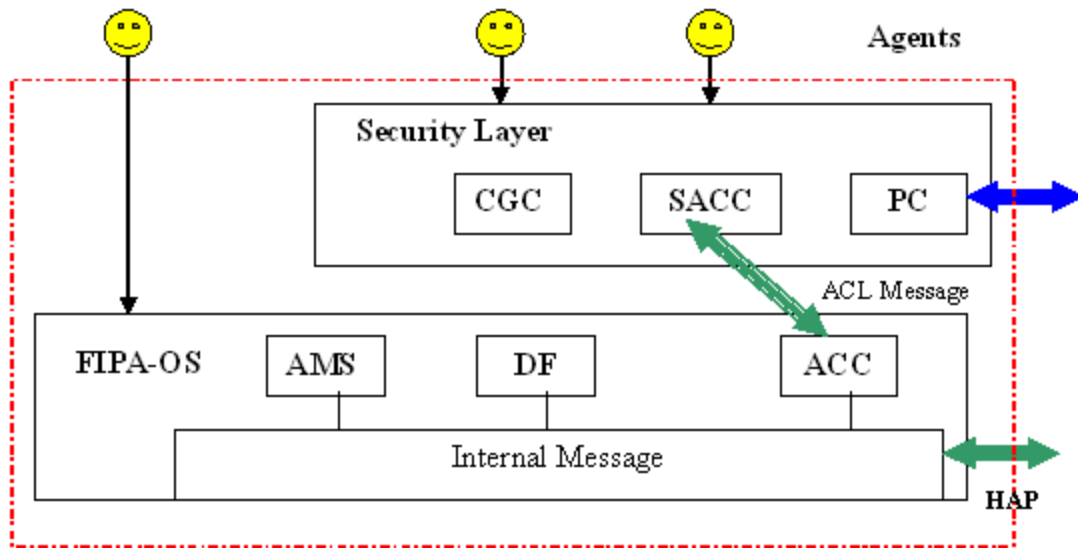


Figure 1. Abstract view of two layer architecture [5].

3.1.3. Trusted Relationships. The security layer and the FIPA-OS layer are considered safe. This includes the functional components along with the internal message communication of the platform. The Certificate Authority (CA) ensures that each platform that is authenticated can be trusted. All communicative interaction between the agent carrying specifications from the Universal Privacy Ontology and the Privacy Component occur over secure communication channels and are also regarded as safe.

The agent trusts its Home Agent Platform (HAP), which consists of the components ACC, AMS and Directory Facilitator (DF) in the FIPA-OS platform layer and SACC, CGC, Authenticator and PC in the security layer along with the internal communication channel. When an agent registers to its HAP, it assumes that its HAP is trustworthy and entrusts its profiles to it. Because this exchange occurs over secure communication channels, the trust relationship cannot be compromised.

Secure Communication Channel remains as discussed in [5], and requires no change to accommodate the Privacy Component therefore an internal description is omitted.

3.1.4. Privacy Component Implementation Algorithm. Authentication and negotiation processes involve the SACC agent, a negotiator agent and protocol objects. The authentication process uses an authentication protocol object, the negotiation process uses a negotiation protocol object, and the privacy exchange process uses a privacy protocol object.

When a SACC agent initiates communication, it sends a request message to the SACC on a remote platform. When the response is positive, the SACC generates a negotiator agent on the local platform. A negotiator protocol object is generated which defines the steps to be followed during the negotiation phase [5]. If a privacy exchange is requested by the initiator, a privacy protocol object is also generated which details the type of communication requested. The privacy

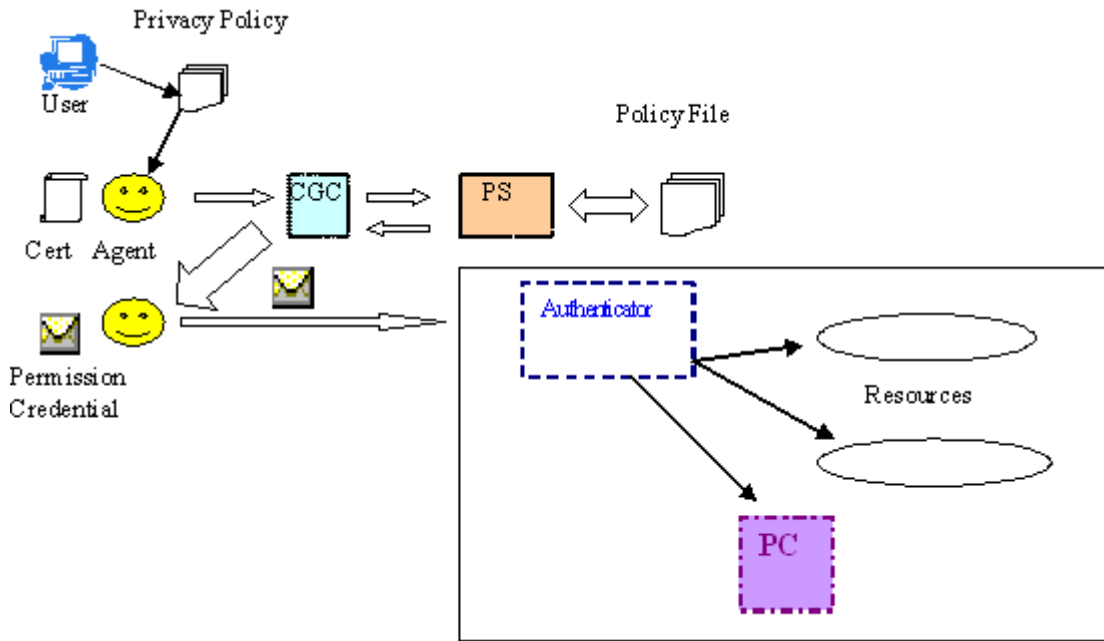


Figure 2. The system architecture [5].

protocol object interacts with the Privacy Component once the authentication process is complete and during the negotiation phase.

Once the authentication process is complete, the negotiator agents on both sides take control of the exchange. The privacy protocol object interacts with the PC. Once the privacy exchange is successful and complete, it issues a “Complete” to the negotiator agent on its respective side. If it is unsuccessful, it issues a message relaying the type of error that occurred. After the negotiation phase is complete, both sides report the final results to the SACCs. If the results are positive, the negotiators provide the necessary certificates, or the shared cryptographic options and secret keys. [5]. In the event of failure, the appropriate messages are reported back to the SACC. Types of errors that may occur are verification of identity fails, unreadable messages occur, the privacy policies are incompatible, time out error or the incoming message does not match the expected error.

4. Phase Two - Universal Privacy Ontology

The principal purpose of the Universal Privacy Ontology (UPO) is to enable agents to exchange privacy related information using a common vocabulary. The UPO will clearly define various types of privacy, for example, privacy of personal behavior versus privacy of communication channels [4]. The UPO must include the core elements defined in the PC, but also include parameters and index terms. The UPO must also be descriptive enough to specify the highest known standards of data protection and privacy [4]. Lastly, the UPO should allow users to specify their privacy preferences to a Web site, but also allow agents to collect and store information about the Web sites and other agents they interact with [4].

The FIPA agent will carry the selected privacy settings derived from the UPO as configured by the user. The user will make selections based on the core data elements of this ontology. These data selections refer to the types of privacy considerations that are acceptable

and at what levels. Additional data elements can be defined by extending the schema but are optional. The agent will carry this configuration for the user until the user changes it. When the configurations are initially set or updated, the agent will notify its HAP and exchange the information with the Privacy Component over secure communication channels. This ensures that the privacy selections will not be compromised.

5. The Complete Picture

The complete process, from the user selecting a privacy policy to the agent receiving authorization to the agent communication with the PC is shown in Figure 2.

Initially the user creates a privacy policy using the UPO. The agent then takes the privacy policy to its HAP and authenticates. This authentication is required for all incoming mobile agents and is performed by the CGC in the security layer of the platform [5]. The agent must provide valid proof of identity in the form of a digital certificate and signature of the owner. Lack of valid proof leads to rejection of the agent's request for a credential.

Once an agent is determined to be legitimate, the CGC consults with the Policy Server (PS) for the appropriate authorizations. The PS is an independent component that manages both platform level and application level policies [5]. This discussion will focus solely on the platform level policies. The PS issues access rights for each agent, based on pre-defined policy criteria, and then the decision is sent back to the CGC. The CGC then creates the credential which includes all permissions authorized for the agent [5] including the right to communicate with the PC.

Next the agent initiates communication with the PC using ACL. It provides the user's privacy policy and any additional privacy policies it wishes to compare (i.e. the privacy policies of several lending institutions). The PC compares the core data elements of the user's privacy policy with its current holdings for the user and makes any updates necessary. The PC then compares the core data elements of the comparison privacy policies and makes determinations based on compatibilities. The PC responds back to the agent with the suitable matches. The agent further analyzes the lenders privacy policies, including any additional data elements independently generated and makes the appropriate selection for the user based on criteria outside the scope of the privacy policy (i.e. is it FDIC insured, are there any hidden fees, points, term of mortgage, etc).

6. Conclusion

Development of the Semantic Web has been hindered in many ways due to the exclusion of privacy rights. Users want tools that are powerful and robust; however users are unwilling to surrender privacy in the process. The tremendous growth of the Internet has made privacy issues front and center. Unless privacy rights and concerns are built into the Semantic Web, users will be reluctant to use it. This research proposal presents a unified approach to incorporating privacy into the Semantic Web.

There are two major components of this proposed solution. Privacy will be addressed by building a Privacy Component into the foundation of agent communication and a Universal Privacy Ontology will be created to interact with the Privacy Component. This Privacy Component is the mechanism and will contain a basic set of data elements for all users. Users

will create a privacy policy using the Universal Privacy Ontology which will allow a user to define additional data elements. FIPA agents will utilize the privacy policy created and interact with the Privacy Component. Use of the Universal Privacy Ontology in conjunction with the two-layer agent architecture will allow the Semantic Web to have the respect of privacy embedded in its foundation.

The significance of this project is in the fact that inclusions of privacy considerations and rights are paramount to the adoption of the Semantic Web. The exploitation of privacy rights in the World Wide Web has made privacy issues front and center. Users are not willing to have their privacy compromised. Privacy must be embedded in the foundation of the Semantic Web in order for it to prosper. There is no privacy provision in FIPA, or in any other standard related to the Semantic Web. By building privacy into its core foundation, users will feel confident in its use. Technological growth will ensue because research and development will no longer be hindered by a lack of adaptability regarding privacy and also because there will now be a uniform and consistent privacy methodology. Researchers and educators will develop new and exciting uses of the vast amounts of data available without infringing on the privacy rights of others. Unique and dynamic ways of forming partnerships among businesses will emerge. Lastly, society at large will benefit from the powerful and robust search tools, having agents plan daily activities, to efficiently find information on the Semantic Web and feel comfortable in knowing that their privacy is being respected.

Inclusion of Rights to Privacy issues are important to further advance technological growth of semantic search and retrieval tools, agent technology, and ontology development tools. This is accomplished all within a framework that incorporates privacy into the foundation of the Semantic Web. Researchers and educators will develop new and exciting uses of the vast amounts of data available without infringing on the privacy rights of others. New and dynamic ways of forming partnerships among businesses will emerge. Users in general will utilize the powerful capabilities of the Semantic Web with confidence in knowing that their privacy remains intact.

7. References

- [1] Foundation for Intelligent Physical Agents. (2002, December 3). In FIPA ACL Message Structure Specification (). Retrieved July 18, 03, from <http://www.fipa.org/specs/fipa00061/SC00061G.html>.
- [2] Golbeck, J., Hendler, J., & Parsia, B. (2003). Trust Networks on the Semantic Web. WWW 2003,.. Retrieved July 14, 03 from <http://mindswap.org/papers/Trust.pdf>.
- [3] Kagal, L., Finin, T., & Joshi, A. (2002). Developing Secure Agent Systems Using Delegation Based Trust Management (AAMAS 2002). Retrieved July 14, 03 from <http://www.cs.umbc.edu/%7Elkagal1/papers/lkagal-developingsecure.pdf> .
- [4] Kim, A., Hoffman, L. J., & Martin, C. D. (2002). Building Privacy into the Semantic Web: An Ontology Needed Now. Paper presented at the meeting of the Semantic Web Workshop, WWW 2002. Retrieved July 16, 03 from <http://SemanticWeb2002.aifb.uni-karlsruhe.de/proceedings/Position/kim2.pdf> .

[5] Zhang, M., Karmouch, A., & Impey, R. (2001). Towards a Secure Agent Platform Based on FIPA. In G. Goos, J. Hartmanis & J. van Leeuwen (Eds.), *Mobile Agents for Telecommunication Applications, Proceedings of the Third International Workshop, MATA 2001* (pp. 277-289). Montreal: Springer-Verlag.