Development of Personal Information Protection Model using a Mobile Agent

Seong-Hee Bae* and Jaejoon Kim**

Abstract—This paper proposes a personal information protection model that allows a user to regulate his or her own personal information and privacy protection policies to receive services provided by a service provider without having to reveal personal information in a way that the user is opposed to. When the user needs to receive a service that requires personal information, the user will only reveal personal information that they find acceptable and for uses that they agree with. Users receive desired services from the service provider only when there is agreement between the user's and the service provider's security policies. Moreover, the proposed model utilizes a mobile agent that is transmitted from the user's personal space, providing the user with complete control over their privacy protection. In addition, the mobile agent is itself a self-destructing program that eliminates the possibility of personal information being leaked. The mobile agent described in this paper allows users to truly control access to their personal information.

Keywords—Information Protect Model, Mobile Agent, Personal Information Protection, Privacy Protection Policy

1. INTRODUCTION

In a ubiquitous environment, there is always the possibility of personal information, even security techniques, being leaked to other people. Therefore, a method is needed that can protect personal information across any network. Until now, people have protected their privacy with methods such as the P3P (The platform for Privacy Preference Project) [1], pawS, E-P3P [2], or with an ID system [3, 4] introduces the general privacy and security management techniques in pervasive computing systems. These methods give a limited number of people access to personal information with various approaches, but must not reveal personal information to the service provider. Therefore, it is not fair to say that personal information is being completely protected.

Since the past and present personal information protection models were dealing with the PC (personal computer), which could not completely protect an individual's personal information, the idea of a mobile agent based system has come about. PC-based server management policy means that when the conditions are met the client gives information of the client to the server to

※ This research was supported by the Daegu University Research Grant, 2009.
Manuscript received February 18, 2010; accepted March 24, 2010.

Corresponding Author: Jaejoon Kim
* Graduate School of Industrial Information, Daegu University, Gyeongbuk, Korea (ksb109@nate.com)
** School of Computer and Communication, Daegu University, Gyeongbuk, Korea (jjkimisu@daegu.ac.kr)

manage.

This paper suggests a method for users to receive services via a mobile agent without having to reveal their personal information. The user who owns the information controls his or her personal information by regulating his or her own privacy policy. When the user needs to receive services that require personal information, he or she will approve what personal information is released in order to receive the service. The service provider is only able to provide the service when the service policy of the user and provider are compatible. Moreover, after the mobile agent has made it possible for the user to receive the service, the program will destroy itself. In this paper, the personal information considered includes every kind of personal information that the user might be required to reveal in order to receive a particular service.

The rest of this paper is organized as follows. First, in section 2, we describe the related works on the privacy policy. We then propose a personal information protection model in section 3. In Section 4, we analyze our comparison results. Conclusions are drawn in Section 5.

2. Related Work

There have been many different privacy protection methods in the past. First, there have been methods implemented by the user. These methods include protecting a personal PC with a firewall, e-mail address protection, erasing web access records, and surfing anonymously. Second, server side methods have been used by companies or groups to protect huge amounts of information. These methods rely on a firewall or a virtual private network. Finally, there is the method of putting a secure space on the server. This method provides privacy by having the server and the user cooperate by using a password system or a P3P. These days, in order to protect personal privacy, a negotiation method is recommended. The most commonly known methods are the P3P, pawS, E-P3P, and an ID system.

2.1 P3P

P3P is a system that automatically compares the website’s privacy policy when a user accesses it. It has been considered a technology that allows the user to control personal information manually by controlling cookies. The website operator monitors who uses the website and what the user does on the website. The user sets his or her privacy policy once he or she is on the website using a corresponding P3P web browser. When they access a site using a corresponding P3P web browser, the website will automatically check the website’s privacy policy and the user’s privacy policy and will only allow access when the two policies match. The P3P system will only allow access when these two policies match and will send a warning message when they do not match.

2.2 pawS (Privacy Awareness System)

The P3P system has a flaw where it cannot be applied to the user’s privacy preference environment. The pawS system [5] is a method that addressed this flaw. When the user goes into an environment where the pawS is being used,

- the privacy beacon will alert the service's proxy URI.
- the user will send the URI if the user has a preference of a personal proxy.
- it will use the personal proxy to compare the website's policy and the user's policy. When the results match, the user will be allowed to access the website.

However, both P3P and pawS systems are methods that enable the service provider to collect personal data. Therefore, it is not fair to say that the user's personal information is being completely protected.

2.3 E-P3P

The E-P3P (The Platform for Enterprise Privacy Practice) is a technology that is being studied at the IBM privacy institute. It has been developed to address problems in the most well known privacy protection technology, the P3P. It is used by companies to ensure privacy for its customers. Thus, this method can protect the user's sensitive personal information. In E-P3P, the privacy policy is activated by subject, purpose, and data categories. For instance, a marketing department can use customer records for e-mail notification or SMS (short message service).

Companies or public institutions offer proposals for the P3P [6] or the E-P3P [7] in order to protect privacy, but it does not mean that the technology always follows the contracts agreed upon [8]. In addition, even though the E-P3P is a technology for companies to store and preserve personal privacy, the owner of the personal information must first give the information to the company to store it safely. Therefore, it is difficult to see how the information is being fully protected.

2.4 ID Management System

User-centric ID Management System enables users to set their own personal information, limit its availability, and safely move it using an additional secure channel. In return for the site storing personal information that is not immediately used, the site can bring personal information at the consent of the user. Thus the site can reduce the burden of managing personal information and since the user provides personal information when he/she wants to, the user can trust the storage and the procedure of use. Also, since personal information can maintain the provided details, post-administration is relatively easy. Recently, by using the identity selector installed on the user side, use of a consistent user experience as well as the ability to respond to threats such as phishing is also available.

The ID Management System is a complex system composed of multiple technologies: AAA (Authentication, Authorization, Audit / Account) technology, P3P technology, password initialization / synchronization technology, SSO (Single Sign On), and LDAP (Light-weight Directory Access Protocol).

Recently several companies are involved in leading projects based on user-centric ID management. Several examples of these projects would be Liberty Alliance's IGF [9, 10] and Concordia, Novell's Bandit, Eclipse Foundation's Higgins, Ping Identity's SourceID [11], Microsoft's NET Passport [12], and ETRI's electronic ID Wallet [13].

3. PIP (Personal Information Protection) Model

In this section, we suggest a method in order to protect privacy more securely without having a service provider controlling and managing a client's personal information by a service provider, the PIP (Personal Information Protection Model).

3.1 Mobile Agent

Unlike the normal agent that uses the network in client/server form to perform a task, the Mobile Agent performs a task by moving the code between systems and the current internal state. The Mobile Agent provides an appropriate solution when network connections are faulty or when the network environment takes on a lot of load. Therefore it can be useful in PDA (Personal Digital Assistant) or HPC (Handheld Personal Computer) like environments, where memory and computing abilities are limited and when most of the time it is not connected to the network. Continuous monitoring for any change in status, operations that cause a lot of network traffic, or performing a combination of several missions on the network can become main tasks for the Mobile Agent. It can also be used in Software Distribution, remote UI (User Interface), or remote error control where rapid communication and interaction are needed. [14]

People act differently in different situations. They can detect the situation in which they are in and act according to that situation. A person's habits are acquired by the rules the person has achieved through their experience. Intelligent agents can also detect the situation in which they are acting and deduct from the situation. The solution to bring the Mobile Agent to realization and a human recognizing a situation are similar to the ontology to detect the operation of a shared situation and based on prior knowledge, reasoning of a current situation can be said to be absolute.

The following features are common features of a Mobile Agent.

- Object Passing: When moving, its own code, data, and travel arrangements are all moved.
- Autonomous: It possesses information of its duties and destination.
- Asynchronous: It has its own tread, and can run independently from other agents (asynchronous)
- Local Interaction: It can communicate with other Mobile Agents and other static objects inside the area and it can dispatch a new Mobile Agent in order to communicate.
- Parallel Execution: In order to perform simultaneous missions, it can send multiple agents to multiple locations to perform them.

Mobile Agents are created and run in separate Runtime Environments and can sometimes move to a different Runtime Environment.

3.2 Personal privacy protection model configuration

The PIP regulates the personal information and data protection policy in the user's personal space. When the user needs to receive services that require personal information, the user will obtain a program itself that will provide the service. Therefore, this process can prevent personal information from being revealed. The configuration of the suggested model is indicated in Figure 1.

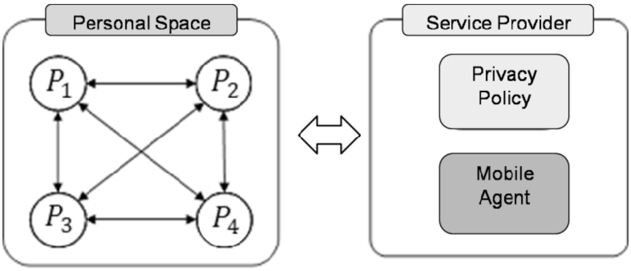

Fig. 1. PIP Model

The following describes the parameter's characteristics.

- Personal Space: The user's space that is made of one or more P_i.
- P_i : is an individual space that is made of personal information and a privacy policy. In this space, the mobile agent can provide the service and exchange info.
- Service Provider: sends the mobile agent to provide the service when it receives a request.
- Privacy Policy: provides the service that will have the conditions the mobile agent needs legally. The P_i will have the extent of personal information that can be revealed and the privacy policy.
- Mobile Agent: A program that provides the service when moved to P_i and is destroyed automatically when finished providing the service.

When the service provider sends the mobile agent to P_i, P_i will compare the privacy policy from the service provider and the user's privacy policy and decide whether or not to accept the service. The overall configuration and processes are shown in Figure 2. The personal data that needs protection is regulated by P_i and is not revealed to the outside. The overall process is divided into two main steps.

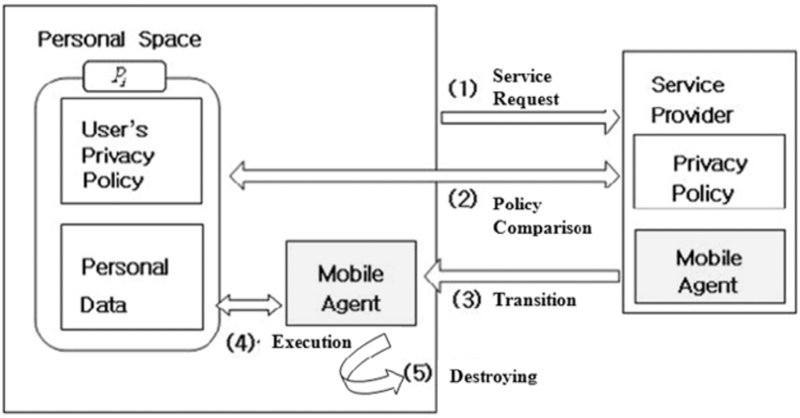

Fig. 2. The overall structure and process for PIP

[Step 1] Service request and comparing privacy policies

1) Service request: One of P_i will request the service.
2) Comparing privacy policies: Compares the service provider's privacy policy and P_i's privacy policy and decides whether P_i can accept the mobile agent.

[Step 2] Moving, executing, and destroying the mobile agent

3) Moving the mobile agent: The service provider will send the mobile agent to each P_i in the personal space.
4) Executing the mobile agent: The moved mobile agent will provide the service by using personal data from P_i.
5) Destroying the mobile agent: After the mobile agent provides the service, the mobile agent will destroy it, therefore eliminating any possibility of the data being used twice or being revealed.

In order to overcome the problem of the owner not controlling user's personal information, the PIP puts the privacy policy and the personal information into P_i and lets the owner control user's personal information, thus preventing any possibility of the information being leaked. The P_i is a digital device where the user can store his or her schedule or location data and regulate personal information from P_i. Giving personal information to anybody is also regulated by P_i. The service provider is not collecting or modifying data but sending a mobile agent to P_i and providing the service. Thus after the mobile agent gives out the service it will destroy itself. Following this process will prevent personal information from being used or revealed.

3.3 Privacy policy

A privacy policy aims to protect personal information by blocking unwanted people from accessing personal information. The service provider also sets a privacy policy to provide services. A privacy policy for protecting personal information and a privacy policy for providing services are identical in shape and are made up of more than one rule. Each rule has one or more conditions and these conditions must be fulfilled in order for the service to be executed as shown in Table 1.

The first column in Table 1 is to distinguish the possessed object and each of the rules. The user's personal information is treated as a distinguishing object by the mobile agent and the service provider. The mobile agent distinguishes whether the purpose of using the personal information is only for executing the service. The secondary use shows when the personal information can be used again and the limits on use when the user is anonymous. The service provider

Tabel 1. Privacy policy

	Object	Usage Selection	Secondary Usage	Usage Period	Behavior
Service request / Service provide	Mobile Agent Service Provider	Service Execution Others	Permission Anonymity Non-permission	Service Execution period Holding period after service	Access permission & transmission

Tabel 2. Attributes for privacy protection policy

Object	Attribute	Value
Client & Provider	AR	OM, OS
	PPD	ES, RE
	SPD	RU, UA, UP
	TU	P_TE, P_KP

also limits requests for anonymous access. The time period is distinguished as when the service is using the personal information and when the service is preserving the personal information. The action follows these conditions and allows the service provider to access and send the mobile agent to P_i.

Table 2 distinguishes the service request and the service supply and is shown as the client and the provider, respectively. The characteristics of the rule are as follows. The AR (Access Receive) shows the open personal information and has the OM (Open Mobile Agent) and the OS (Open Server). The OM limits the open personal information to the mobile agent and the OS limits the service to the server. The PPD (Purpose of using Personal Data) shows the purpose of the use of the personal information and has the ES (Execute Service) and the RE (Request Etc). The ES means that the service has been executed as requested and the RE shows that there is another intention other than executing the service.

The SPD (Secondary use of Personal Data) covers the secondary use of the personal information. In characteristics it has the RU (Reject Use), the UA (Use Anonymous), and the UP (Use Permission). The RU rejects the request to use the personal information a second time and shows that the service provider has not requested a secondary use. The UA allows the service to use the personal information a second time but only when it is anonymous. The UP allows complete access to the personal information a second time and shows the service provider's complete secondary use request. In case the client owns the UP, the provider can have any one of the RU, UA, or the UP in order to make an agreement. However if the client has the RU, the provider must also have the RU, and when the client has the UA, the provider must have either RU or UA in order to make an agreement.

The TU (Term of Use) shows the period of the use of personal information and has the P_TE (Permission_Term of Execute service), P_KP (Permission_Keep Personal data). The P_TE shows that the personal information is in use in the service and the P_KP shows that the provider still has the information after the service has been executed. By the rule in Table 2, the client has the right to allow the mobile agent to access his or her own P_i and the provider has the right to send the mobile agent.

4. Application of the PIP model

In order to examine the possibility of implementing the proposed model, we applied it to a mental disease diagnosis service scenario. In this section, we also describe the system configuration, privacy policy comparison, and comparison results.

4.1 Mental disease diagnosis service scenario

4.1.1 System configuration

The overall configuration of the system in the service is shown in Figure 3. In Figure 3, the Personal Space is Mr. A's personal PC (Personal Computer) and the Service Provider is S hospital that is providing the mental disease diagnosis service. In order for the service to take place, the next section compares Mr. A's privacy policy and S hospital's privacy policy.

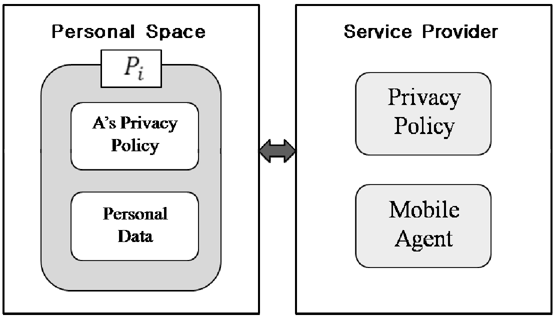

Fig. 3. System configuration of a service scenario

4.1.2 Creation and comparison of privacy policy

The privacy policy for the protection of the user's personal information consists of the rules in Table 2, rules of service request and service supply. (Table 3) The C_02 rule is Mr. A's policy for a service request and the P_02 rule is the S hospital's policy to provide the service. Looking at the C_02's and the P_02's characteristic on the PPD, we see that the ES and the RE do not match. We also note that with the SPD, the RU and the UA do not match. Mr. A's purpose of personal information use is to execute the service and does not allow secondary use of the information. However, S hospital has another purpose other than providing the service and is asking Mr. A to allow secondary use of personal information with anonymity. Therefore, the rules of the C_02 and the P_02 do not match so the service cannot be provided. In this example, Mr. A and S hospital will be notified that the service cannot be provided.

Mr. A receives a message that the characteristics of the PPD and the SPD do not match. So he changes his policy to allow his personal information be used a second time with anonymity. After he changes his policy, he requests the service again. (Table 4) However S hospital's purpose in using the personal information characteristic PPD is still set to RE and does not match

Table 3. Service requests and privacy protection policy for a scenario

Rule number	Object	Attribute			
C_02	Client	AR=OM	PPD=ES	SPD=RU	TU=P_TE
P_02	Provider	AR=OM	PPD=RE	SPD=UA	TU=P_TE

Table 4. Modified service requests and privacy protection policy for a scenario

Rule number	Object	Attribute			
C_03	Client	AR=OM	PPD=ES	SPD=UA	TU=P_TE
P_02	Provider	AR=OM	PPD=RE	SPD=UA	TU=P_TE

Mr. A's ES. Therefore, Mr. A must make a decision about whether to allow S hospital to use his personal information for a different purpose in order to gain access to the service. Mr. A decides not to change his PPD characteristic and instead try to find the service at another hospital.

4.1.3 The procedures to execute the service

Figure 4 describes the system configuration and service sequences.

(1) Mr. A requests a mental disease diagnosis service from S hospital through his PC.
(2) S hospital and Mr. A compare each other's policies. Messages are sent to S hospital and to Mr. A to inform them that the characteristics of their policies do not match. Mr. A changes his own policy and asks for the service again.
(3) However, since the policies still do not match, Mr. A withdraws his request and requests the service from another hospital.

Mr. A chooses to withdraw his service request from S hospital and to request the service from another hospital because he did not want his personal information to be used for a purpose other than receiving the service.

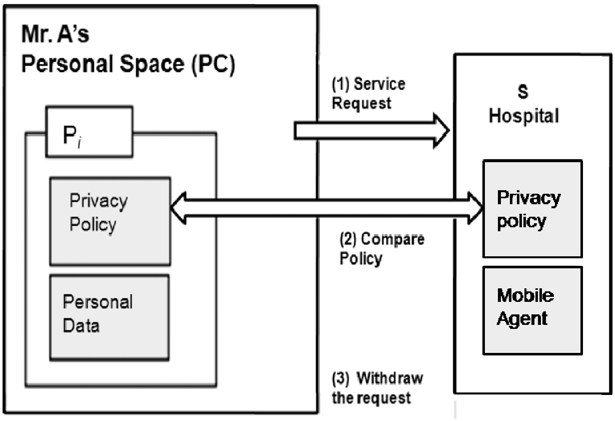

Fig. 4. The system configuration and service sequences

Table 5. Authentication and Authorization Levels

	P3P	pawS	E-P3P	ID management system	PIP
(1)	X	X	X	○	○
(2)	X	X	X	△	○
(3)	○	○	○	X	X
(4)	○	○	○	○	○

Note. (1) Personal information protection policy by information owner, (2) Personal information management by information owner, (3) Personal information protection policy by service provider, (4) Personal information management by service provider. In the ID Management System the triangle means that though the individual can control their own privacy policy, the service provider can still manage the policy.

4.2 Results and discussion

Personal information protection technology by the owner allows the information owner to control access is possible in an ID system and a PIP because the owner is in charge of his or her own policy settings.

What we have thought of as ‘personal information control by the owner’ has involved the owner controlling his or her own personal information with an ID system. The problem is that when the owner makes an ID account, the personal information that went into the ID account is collected by the service provider. However, with the PIP method, the owner controls his or her own personal information and the service provider does not collect the information. This is a fundamental change in the control over access to personal information.

When we consider ‘personal information protection policies by the service provider’, we see that the service provider is describing the personal information protection policy under a certain standard. Methods other than the ID system and the PIP rely on the service provider to control the information protection policy.

‘Personal information management by the service provider’ includes every kind of method in which the service provider manages personal information. Under the PIP method, the owner of the information manages the information and may decide to grant permission to the service provider to also use or control the information. Table 5 summarizes the comparison results based on different methods.

5. CONCLUSION

The PIP (Personal Information Protect) model prevents the service provider from leaking personal information or from permitting unwanted secondary usage of the information. In order for a user to receive a service, the PIP model uses a mobile agent. The mobile agent compares privacy policies and decides whether to receive the service or not. It is similar to the ID system, but it has addressed the current problem of protecting personal information by placing control over access to the information in the user’s personal space. In addition, personal information can be protected more securely since the mobile agent destroys itself after it has given out the service.

Therefore, the PIP model solves the privacy violation issue while protecting personal information. Another matter that is worth investigating is how the different policies will be compared before receiving the mobile agent and how the two policies will make an agreement when the policies do not match. In addition, there must be real data simulations.

REFERENCES

[1] "P3P1.0: The Platform for Privacy Preferences 1.0 Specification," W3C, http://www.w3.org/TG/P3P/, 2002.

[2] P. Ashley, S. Hada, G. Karjth, M. Schunter, E-P3P, "Privacy Policies and Privacy Authorization," ACM Workshop on Privacy in The Electronic Society (WPES), pp.103-109, 2002.

[3] "Identity Management Systems (IMS): Identification and Comparison Study," Commissioned by the Joint Research Centre, Seville, Spain, September 2003. http://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf.

[4] Kurkovsky, O Rivera, J Bhalodi, "Classification of Privacy Management Techniques in Pervasive Computing," International Journal of u- and e-Service, Science and Technology, Vol.11, No.1, pp.55-71, 2007

[5] Michiru Tanaka, Jun Sasaki, Yutaka Funyu, and Yoshimi Teshigawara, "A Personal Information Protection Model for Web Applications by Utilizing Mobile Phones," Frontiers in Artificial Intelligence and Applications; Proceedings of the 2008 conference on Information Modelling and Knowledge Bases XIX, Vol.166, pp.346-353, 2008.

[6] Md. Nurul Huda and Eiji Kamioka, "Privacy Protection in Mobile Agent based Service Domain," Proceedings of the Third International Conference on Information Technology and Applications (ICITA'05), Vol.2, pp.482-487, 2005.

[7] M. Langheinrich, "A Privacy Awareness System for Ubiquitous Computing Environments," Proceedings of International Conference on Ubiquitous Computing 2002 (UbiComp 2002), pp.237-245, 2002.

[8] Xiaodong Jiang, Jason I. Hong, James A. Landay "Approximate Information Flows: Socially-based Modeling of Privacy in Ubiquitous Computing", Proceedings of the 4th international conference on Ubiquitous Computing, Sep., pp.176-193, 2002.

[9] "Introduction to the Liberty Alliance Identity Architecture," Liberty Alliance Project, http://www.Projectliberty.org/, March, 2003.

[10] Scott Cantor, John Kemp, "Liberty ID-FF Protocols and Schema Specification," Version 1.2 Liberty Alliance Project, January, 2004.

[11] "SourceID: Federated identity infrastructure," Ping Identity, 2004, http://www.sourceid.org/.

[12] "Microsoft .NET Passpost, "Microsoft, 2004, http://www.microsoft.com/net/services/passport/.

[13] S.R. Cho and S.H. Jin, "A Digital Identity Interchange Framework for User-Centric ID Management," http://eettrends.etri.re.kr, Vol.23, No.6, pp.102-111, December, 2008.

[14] Xiang Yang, Yuanyi Zhang, Qinzhou Niu, Xiaomei Tao, Luo Wu, "A Mobile-Agent-Based Application Model Design of Pervasive Mobile Devices," Proceedings of Pervasive Computing and Applications, pp.1-6, 2007.

Seong-Hee Bae

She received her B.S. degree in the Department of Landscape Architecture from Daegu Catholic University and her M.S. in the Graduate School of Industrial Information from Daegu University in 1994 and 2008, respectively. She is interested in ubiquitous security and personal protection policy areas.

Jaejoon Kim

He received his B.S. degrees in Mathematics and Electronics Engineering from Hanyang University, Korea in 1988 and 1990. He received his M.S. and Ph.D. degrees in the Department of Electrical Engineering in 1995 and 2000, respectively. From 2001 to 2002, he worked for the Electronics and Telecommunications Research Institute (ETRI) in Korea. Currently, he serves as an associate professor at Daegu University. His research interests include multimedia codec, image processing, and nondestructive evaluation.