A Study on Policy-based Access Control Model in SNS

Kyong-jin Kim[1*], Seng-phil Hong[1**] and Joon Young Kim[2]

[1]*Sungshin Women's University*, [2]*KUDOS Co., Ltd*
[1]*{kyongjin, philhong}@sungshin.ac.kr*, [2]*jkim@kudos.co.kr*

[*] *First author*, [**] *Corresponding author*

Abstract

Security and privacy have emerged as important issues owing to the proliferation of social networking site. Sharing and distribution of relationship-based information on social network sites can have a serious impact on an individual's activity; moreover, it can exert a negative influence on the overall information society. To solve security and privacy issues of social networking, we introduce a policy-based access control model to support access control based on privacy policies. Our system helps to protect users from potential dangers in social network environments. This work examines the practical applicability of the model by prototyping the system implementation method in the web environment. We also compare our research with other studies on privacy protection for social networks.

Keywords: *Privacy, Social Networking Services, Access Control, Privacy Policy*

1. Introduction

With the spread of new technologies such as location-based systems and smart phones/pads, frequency of usage of social network sites (SNS) has increased sharply. The latest report on the growth of social networking [12] suggests that it accounted for nearly 1 in every 5 minutes spent online globally in October 2011, and reaches 82% of the world's Internet population (see Figure 1).

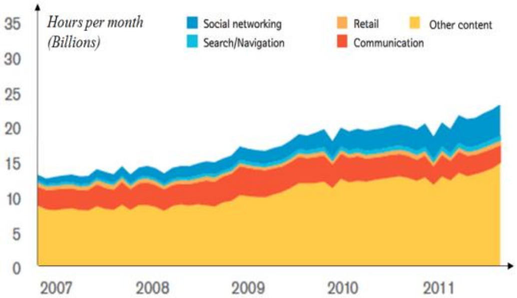


Figure 1. **Status of social networking**

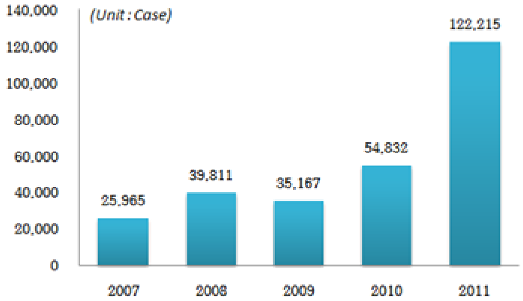


Figure 2. **Cases of privacy breaches**

On the other hand, there is great concern over the dangers of social networking. According to a Sophos report [8, 10], 61% of respondents said that Facebook poses the biggest security risk on the internet. In other words, there are a wide variety of threats including spam, phishing, or malware attacks via social networks, as well as many potential personal issues should individuals' profiles be breached. According to the Korea Internet & Security Agency [5], the number of privacy breaches involving SNS increased to 122,215 last year from 54,832 the previous year, as shown in Figure 2. According to these records, the public sharing and distribution of personal data led to the disclosure of details including addresses and personal relationships. Therefore, it is very important to understand the associated privacy policies on SNS. To address this issue, we introduce an access control model (PACM) to support the privacy policies of social network environments.

2. Related Works

With SNS usage booming, concerns about the easy access to personal information have also risen. In this section, we briefly discuss other security proposals. There are several works concerning SNS related to security policies. In order to protect personal information from being publicly shared, Facebook [8] provides various security and privacy settings. These are designed to help users protect their personal information and accounts. Schneier [6] discussed and compared some of the existing self-management mechanisms of three social networking applications, namely Facebook, MySpace, and LinkedIn. His work suggested different aspects for dealing with trust. However, their approach disregarded important privacy policy settings in SNS. Our approach presents a systematic and comprehensive privacy policy based on the purpose, condition, and role of the user (these terms are defined in Section 4). Choi [2] suggested a model based on a Privacy-policy Management (PpM) Server, which allows access to shared personal information to be controlled by the owners of that data. However, Choi did not consider role-based access control (RBAC) features, such as permission based on roles and constraints. In comparison, our work supports RBAC[7, 11] and can restrict anonymous or unauthorized access to personal. Geng et al. [3] presented a personalized privacy management framework that allows users to participate in privacy management. Their proposed approach uses text analysis to classify the privacy policies. They claimed that their framework makes privacy policies easier to read and understand than the existing presentation. Even though their approach mainly attempted to specify privacy policies, it is difficult to clearly separate different policies. In this paper, our approach illustrates a secure access control model based on the privacy policies of social networks.

3. Motivation

Many people even avoid SNS for fear of more serious threats, namely the theft and misuse of their personal information. Given the rising popularity of SNS, issues of security and privacy are becoming more important [1, 4, 6]. In particular, social networking relationships between people have led to dangers involving individual profile breaches and the unwanted access of personal data. We can classify the privacy issues of social networks as either identity issues, policy issues, or access control issues. We have analyzed the factors behind each of these issues, and present the associated threats and vulnerabilities in Table 1.

Table 1. Analysis of privacy issues related to SNS

Issues	Factors	Threats and vulnerabilities
(1) Identity issues	Weak authentication	SNS performs weak authentication based on a single username and password
	Identity theft (e.g., fake profile)	False profiles are used for advertising or marketing within a particular network of friends
	Difficulty of complete account deletion	Although it is easy to remove their primary pages, secondary information such as public comments on other profiles cannot be completely deleted

(2) Policy issues	Ambiguity of policy wording	Privacy policies tend to be vague in specifying what is and what is not personal information
	Vulnerability to user carelessness	Users' privacy may be under even greater threat from images posted by others
		There is often a tendency to accept friend requests without checking their authenticity or suitability
(3) Access control issues	Ease anonymous access	Anyone with a valid e-mail address can join any network
		Unknown people can access public profiles
	Secondary data collection	Private information is directly accessible by profile browsing
		Lack of transparency about certain data collection practices by allowing searches
	Negative or hostile use of data without consent	Information disclosed can be used for negative service purposes such as targeting and the transfer of data to third parties
		Hostile users can retain information from SNS profiles for negative use

To overcome these issues, we suggest a policy-based access control model to solve the issues of the protection of privacy.

4. Policy-based Access Control Model (PACM)

Our proposed PACM aims to protect the privacy of its users' personal information. It securely manages private information, and helps to control secure access to authorized users based on privacy policies. PACM consists of three distinct parts: an Integrated Authentication Mechanism (IAM), an Access Control Handler Mechanism (ACHM), and a Privacy Policy Controller Mechanism (PPCM). An overall view of the system is shown in Figure 3.

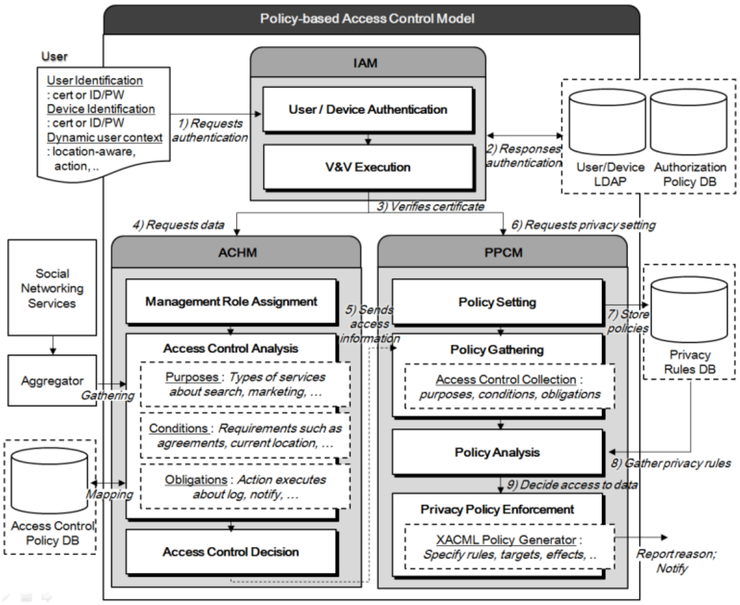

Policy-based Access Control Model
User
User Identification
: cert or ID/PW
Device Identification
: cert or ID/PW
Dynamic user context
: location-aware, action, ..
1) Requests authentication
IAM
User / Device Authentication
V&V Execution
2) Responses authentication
User/Device LDAP
Authorization Policy DB
3) Verifies certificate
4) Requests data
6) Requests privacy setting
ACHM
Management Role Assignment
Access Control Analysis
Purposes : Types of services about search, marketing, …
Conditions : Requirements such as agreements, current location, …
Obligations : Action executes about log, notify, …
Access Control Decision
Social Networking Services
Aggregator
Gathering
Mapping
Access Control Policy DB
5) Sends access information
PPCM
Policy Setting
Policy Gathering
Access Control Collection : purposes, conditions, obligations
Policy Analysis
Privacy Policy Enforcement
XACML Policy Generator : Specify rules, targets, effects, ..
7) Store policies
Privacy Rules DB
8) Gather privacy rules
9) Decide access to data
Report reason; Notify

Figure 3. PACM

In this model, the IAM is based on identifying the user and the mobile device, such as a cellular phone, a smartphone, or a tablet PC. This is a method of identification that combines user authentication based on certificates or a username/password with device authentication based on dynamic information. The dynamic information, called context information, relates to the user's current activity and location, and may be aggregated. This authentication method may involve verifying whether a mobile device is suitable for SNS, in terms of reliability, as a prerequisite to allowing access to disclosed personal information on the SNS.

The ACHM is given authority according to that of the authenticated user through the IAM. Access control is enabled based on the role, purpose, and condition defined below. A role is dynamically assigned to a user depending on their authentication factors. In order to apply this mechanism to SNS, we have identified the following features:

- A set U of *users*, u is an individual who can use online SNS
- A set R of *roles*, r is a group of authorizations and responsibilities based on common properties; here, the role may or may not be 'friends'
- A set Pu of *purposes*, p_u is the type of service, such as 'search' and 'marketing'. It contains privacy policies with regard to collection, use, sharing, etc.
- A set C of *conditions*, c is defined as an essential requirement that must be met or fulfilled by privacy rules, policies, and guidelines
- A set D of *data*, d is defined as a user's personal information such as profile page, status
- A set O of *obligations*, o must be performed after an access action is executed
- The set of Privacy Constraints $PC = \{(p_u, c) \mid p_u \in Pu, c \in C\}$, pc satisfies the privacy requirement given by r
- The set of Privacy Access Permissions $PAP = \{(pc, d, o) \mid pc \in PC, d \in D, o \in O\}$

The requirements relationship of these features can be defined as follows:

- User Assignment $UA \subseteq U \times R$, a many-to-many function users to role assignment relation; u is a member of r
- Privacy Access Permission Assignment $PAPA \subseteq R \times PAP$, a many-to-many function mapping permissions to role assignment relations; r is given $pap \wedge pap$ requests to access d (if d is released to u) $\Rightarrow r$ is authorized to access d

In this case, data is defined as the information disclosed by a user, such as their interests, preferences, or other private information, and it is important that this is classified by importance. Table 2 presents our proposed hierarchy of information importance.

Table 2. Classification type of personal information

Level	Description
Private data	Critical personal data that is associated with registration information
Restricted data	Users should be informed before this data is disclosed to selected parties
Semi-public data	This should not be disclosed to anonymous visitors, but is freely available to selected parties(friend groups)
Public data	Public data made accessible by all SNS, including to anonymous visitors

The PPCM securely manages the personal data disclosed by a user in the social network environment. The purpose of collecting personal or sensitive information is clearly stated by SNS, and it is important to gather a minimum level of data on SNS users. Unique identifying information, such as a social security number, is not stored, or, in the case of Korea, is only used for encryption. Korea's privacy law is contained in the Personal Information Protection Act (PIPA) 2011. This includes a requirement that the individuals involved must be notified in case of a data breach. For this reason, the PPCM proposed in this paper issues privacy notices when such events occur. In addition, a user can set up a privacy policy for their desired security level, and this is automatically managed when making, using and collecting personal data. The privacy policy in this mechanism is built on XACML [9]. This policy document indicates the status of access control and specifies the privacy protection policies.

5. Prototype implementation

5.1. Algorithm

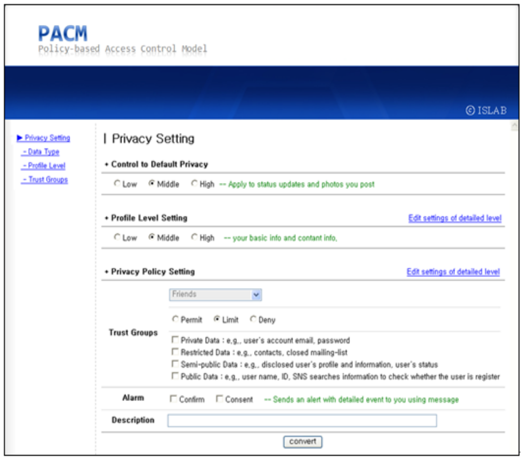
Based on the model described in the previous section, we design the mechanism for the main composition module; the key point of our algorithm is that a mechanism protects personal information using the access control and privacy policies.

Algorithm Policy-based access control

```
if $u \in U \wedge$ isValidating($u_{cert}$, $dev_{cert}$) then
    $resultAuth \leftarrow$useMember($u$);
end if
if $resultAuth$ = true $\wedge$ request $d$ then
    if select $d \in D$ then
        for each $r_i \in R$ do
            if isEqualAuth($r_i$, $u$) then
                $r_{uid} \leftarrow$ assignRole($r_i$, $u$);
            end if
        end for
        if isSuitable($r_{uid}$) $\wedge$ use $p_u \in Pu$ then
             for ($c \leftarrow$ hasConditions($r_{uid}$, $p_u$)) $\neq$ null do
                addRole($c$);
             end for
        end if
        if ($pc \leftarrow$ constraints($p_u$, $c$)) $\in$ PC $\wedge$ isSatisfied($pc$) then
            $pap \leftarrow$ decideAccess($pc$, $d$, obligation ($r_{uid}$ , $pc$));
        end if
    end if
end if
if $pap \neq$ null $\wedge$ isMatchedRules($pap$) then
    switch $pap.auth$
        case permit:
            $papa \leftarrow$ grant access to requested $d$;
        case restrict:
            if $pap.c \neq$ null then
                if performCondition($u$, $pap.c$) = true then
                    $papa \leftarrow$ grant access to requested $d$;
                end if
            end if
            if $pap.o \neq$ null then
                if $pap.o \in N$ then   /* $N \leftarrow \{warning, confirm, alert, consent\}$ */
                    performObligation ($u$, $pap.o$);
                end if
            end if
        case deny:
            $papa \leftarrow$ deny access;
    end switch
end if
```

5.2. Prototype

To demonstrate the feasibility of our model, we implement a prototype that provides protection for personal data and prevents the abuse of disclosed sensitive data in a real system environment. In order to provide privacy management based on access control, users operate an on-screen interface to set an appropriate privacy policy. Figure 4 shows that users can choose the trust group, which helps to set a user's privacy policies and access control settings. This privacy setting shows detailed security information that makes accessing an open network safer. Using the button located at the bottom of the interface, it can convert a machine-readable XML format, known as XACML (see Figure 5).


PACM
Policy-based Access Control Model
© ISLAB
▶ Privacy Setting
- Data Type
- Profile Level
- Trust Groups
Edit settings of detailed level
Edit settings of detailed level
convert

| Privacy Setting

• Control to Default Privacy

○ Low ● Middle ○ High -- Apply to status updates and photos you post

• Profile Level Setting

○ Low ● Middle ○ High -- your basic info and contant info.

• Privacy Policy Setting

Trust Groups: Friends

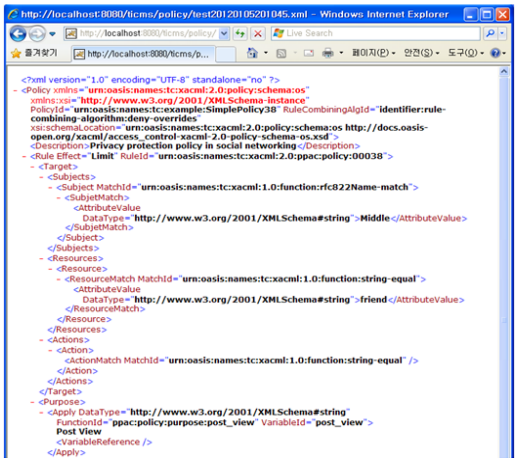
○ Permit ● Limit ○ Deny

□ Private Data : e.g., user's account email, password
□ Restricted Data : e.g., contacts, closed mailing-list
□ Semi-public Data : e.g., disclosed user's profile and information, user's status
□ Public Data : e.g., user name, ID, SNS searches information to check whether the user is register

Alarm: □ Confirm □ Consent -- Sends an alert with detailed event to you using message

Description:

Figure 4. Setting up the privacy policy


http://localhost:8080/ticms/policy/test20120105201045.xml - Windows Internet Explorer
http://localhost:8080/ticms/policy/
Live Search
즐겨찾기
http://localhost:8080/ticms/p...
페이지(P)
안전(S)
도구(O)

```
  <?xml version="1.0" encoding="UTF-8" standalone="no" ?>
- <Policy xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    PolicyId="urn:oasis:names:tc:example:SimplePolicy38" RuleCombiningAlgId="identifier:rule-
    combining-algorithm:deny-overrides"
    xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os http://docs.oasis-
    open.org/xacml/access_control-xacml-2.0-policy-schema-os.xsd">
    <Description>Privacy protection policy in social networking</Description>
  - <Rule Effect="Limit" RuleId="urn:oasis:names:tc:xacml:2.0:ppac:policy:00038">
    - <Target>
      - <Subjects>
        - <Subject MatchId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match">
          - <SubjetMatch>
              <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">Middle</AttributeValue>
            </SubjetMatch>
          </Subject>
        </Subjects>
      - <Resources>
        - <Resource>
          - <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">friend</AttributeValue>
            </ResourceMatch>
          </Resource>
        </Resources>
      - <Actions>
        - <Action>
            <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal" />
          </Action>
        </Actions>
      </Target>
    - <Purpose>
      - <Apply DataType="http://www.w3.org/2001/XMLSchema#string"
          FunctionId="ppac:policy:purpose:post_view" VariableId="post_view">
          Post View
          <VariableReference />
        </Apply>
```

Figure 5. Convert XACML document

6. Performance evaluation

Existing systems use a privacy policy and access control, making it difficult to manage personal information in dynamic relationships. In contrast, our work supports access control based on the role, purpose, and condition, and provides privacy policies for SNS. Our proposed model securely manages the personal data and details being shared throughout the social networking environment. Based on the prototype of the previous section, the security evaluation criterion was applied to the authorization, access control, and policy settings. As shown in Table 3, our work is compared and analyzed against others [2, 3, 6] with regard to privacy policies and access controls in social network environments.

Table 3. Comparative analysis

Security factors	Related works	Schneier [6]	PpM [2]	Jianning Geng [3]	PACM
Authentication	Certificate-based		√		√
	Using dynamic context				√
Access control	Authority based on data type	√			√
	Requirements based policies	√		√	√
Policy setting	Comply with laws		√	√	√
	Automatic convert			√	√
	Self-management		√	√	√

We design a program to simulate its performance. It is given which demonstrates the safety probability of the users' private information. Our simulation result is expressed by the graph of Figure 6. As shown in Figure 6, the number of users can be a value between 100 and 1000, and two lines in the graph represent that they allowed the same number of users to access data. Compared to the system based on existing policies, the PACM system shows better security performance, since our system is restricted to users through privacy policies.

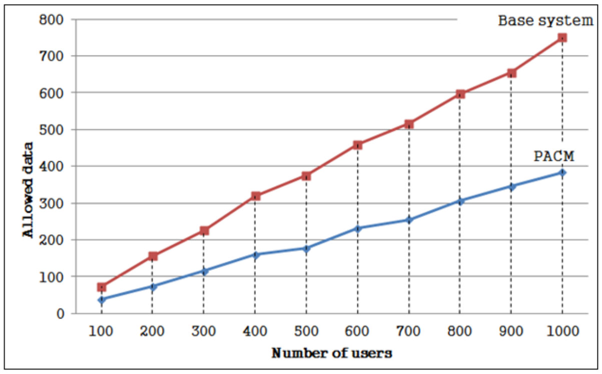


Figure 6. Graph of the security performance

7. Conclusion and Future Work

In this paper, we discussed security-related issues as well as the status of SNS. To address the security and privacy problems of SNS, we have proposed the PACM for securely accessing personal data. Our model protects privacy based on access control, and it supports security features including integrated authentication and privacy policies. It also helps to provide security in social networking environments.

Future studies will continue to focus on the design and development of our suggested model, and we will investigate how personal issues and data can be protected in SNS.

Acknowledgements

This work was supported by the Sungshin Women's University Research Grant of 2012.

References

[1] Korea Communications Commission, Smart Mobile Security Plan **(2010)**.

[2] H.-C. Choi, "A Study on Access Control based on the Policy for Privacy Protection in the Social Media Environment", Internet and Information Security, vol. 1, no. 2, **(2011)**, pp. 46-70.

[3] J. Geng, L. Liu and B. R. Bryant, "Towards a Personalized Privacy Management Framework", Proceedings of SESS'10 **(2010)**.

[4] Korea Communications Commission, KCC's 10-point guideline **(2010)**.

[5] Korea Communications Commission, the number of personal information invasion case, e-National indicators **(2012)**.

[6] B. Schneier, "A taxonomy of social networking data", IEEE Security & Privacy, vol. 4, no. 8, **(2010)**.

[7] Q. Ni, A. Trombetta, E. Bertino and J. Lobo, "Privacy management: Privacy-aware role based access control", Proceedings of the 12th ACM SACMAT '07, **(2007)**, pp. 41-50.

[8] N. O'Neill, "The 10 Facebook Privacy Setting You Need To Know", All Facebook, Available at www. Allfacebook.com **(2011)**.

[9] OASIS, OASIS: Extensible access control markup language(XACML) V2.0. OASIS Specification, Available at www. Oasis-open.org/committees/xacml **(2005)**.

[10] Security Threat Report: 2010, Sophos **(2010)**.

[11] D. Abi Haidar, N. Cuppens-Boulahia, F. Cuppens and H. Debar, “An Extended RBAC Profile of XACML”, Proceedings of SWS’06 **(2006)**.

[12] ComScore’s 2011 Social Report: Facebook Leading, Microbloggin Growing, World Connecting, ComScore, Inc., **(2011)**.

Authors

Kyong-jin Kim

Kyong-jin Kim received her B.S. degree and M.S. degree in Computer Science from Sungshin Women's University. Currently she is studying for her Ph.D. course at Sungshin Women’s University, and she is majoring in Information Protection. She research interests include access control, privacy protection, and security framework.

Seng-phil Hong

Professor Seng-phil Hong received his BS degree in Computer Science from Indiana State University, and MS degree in Computer Science from Ball State University at Indiana, USA. He researched the information security for PhD at Illinois Institute of Technology from 1994 to 1997, He joined the Research and Development Center in LG-CNS Systems, Inc since 1997, and he received Ph.D. degree in computer science from Information and Communications University in Korea. He is actively involved in teach and research in information security at Sungshin Women’s University, Korea. His research interests include access control, security architecture, Privacy, and e-business security.

Joon Young Kim

Dr. Joon Young Kim received his BA degree in Economics from Yonsei University, and BEc degree in Finance from Macquarie University, Sydney Australia. Dr. Kim received MA degree in Economics from Yonsei University. He received Ph.D. in Economics at Claremont Graduate School, Claremont California in 2006. His major is Industrial Organization and Public Choice in Microeconomics. He was a faculty at University of Southern California as a research assistant professor for the Center for Communications Law and Policy and Center for Asian Pacific Leaderships. He had hosted two series of ‘Symposium for Telecommunications Regulations’ during his tenure at USC having most of former FCC Chief economists and prominent scholars such as Jerry Hausman, Simon Wilkie, Nicholas Economedies, Philip Weiser, and Michael Riorden. He served as a senior economist at SK Research Institute and actively involved various research societies for telecommunications and broadcast media. Currently, he is the Managing director at Kudos financial research institute.