Patronus: Augmented Privacy Protection for Resource Publication in On-line Social Networks

Lin Zhang, Yao Guo, Xiangqun Chen
Key Laboratory of High-Confidence Software Technologies (Ministry of Education),
School of Electronics Engineering and Computer Science, Peking University, Beijing, China
{*zhanglin08, yaoguo, cherry*}*@sei.pku.edu.cn*

***Abstract*—With the popularity of on-line social networks and the wide spread of smart phones, it is becoming more and more frequent and convenient for individuals to share resources, such as status, micro-blogs, blogs, photos, videos, and so on, with their friends over on-line social networks. Since on-line resources might be involved with several users at the same time, it is far from enough to protect the privacy of users with the simple group-based access control model (GBAC), in which only the privacy requirements of the resource owner is regarded. In order to provide augmented privacy protection for resource publication in on-line social networks, this paper proposes the concept of resource involvers and a new access model named Patronus, in which, the privacy requirements of the resource owner and its corresponding involvers are both taken into considerations. In Patronus, we employ a simplistic specification based on the format of "when-where-who-what" to describe a resource and the privacy requirements of an individual user. We implemented a prototype application based on Patronus for photo sharing on Android, and demonstrated its feasibility and effectiveness with several case studies.**

***Keywords*-on-line social networks;privacy;resource owner and resource involvers**

I. Introduction

On-line social networks are playing an important role in our daily lives in the modern society. Individual users provide plenty of personal information items in their profiles, such as name, gender, age, birthday, email address, phone number, current university/company, political views and so on. Since some of these items are sensitive, access control is widely employed in order to protect the privacy of users. Generally speaking, each user can classify his/her friends into groups(a typical classification could be close-friends, friends, classmates, schoolmates, colleagues and acquaintances), and then assign different permissions with different groups for different information items.

In addition to personal information items, individuals also post resources in on-line social networks, such status, micro-blogs, blogs, photos, videos and so on, to share with their friends. Sensitive information might be inferred by taking advantages of a certain resource or several resources together. An article in *Hong Kong Economic Times* of September 26th 2011 listed a series of case studies about privacy leakages caused by resource publication on the website of Facebook. We summarized these case studies and propose the following scenario as our motivating example. In a singles party, Alice took a picture of Lucy, Kate and Bob when they clinked, and uploaded this photo on her Facebook homepage to share with her friends. Unfortunately, Lucy did not want others to know her attendance at this party. In this circumstance, the privacy requirements of Alice, who is the owner of the photo, could be preserved as usual; but the privacy requirements of Lucy was not satisfied since she did not have control over the photo publication. To address this problem, we introduce the concept of *resource involvers*, and take the privacy requirements of resource involvers into consideration for resource publication in on-line social networks.

In order to satisfy the privacy requirements of both resource owner and resource involvers, the following questions need to be answered:

- How to identify the involvers with a certain resource?
- How does an involver specify his/her privacy requirements?
- How do we enforce the privacy requirements of the resource owner as well as resource involvers?

In this paper, we proposes a new access model named Patronus for resource publication in on-line social networks. As we know, the 4A theory in on-line social networks indicates that anyone can post anything at any time in any place, so that we can describe a certain resource in the format of "who-what-when-where". Users can also specify their privacy requirements in the same format to indicate what kinds of resources are allowed/disallowed to publish in on-line social networks. We implemented a prototype of Patronus for photo sharing on Android, and demonstrated its feasibility and effectiveness with several case studies.

This paper makes the following main contributions:

- We introduce the concept of *resource involvers* to enlarge the traditional scope of privacy protection.
- We propose a new access model named Patronus to organize the roles, the resource involvers, the privacy policies together in order to provide better privacy protection for resource publication in on-line social networks.
- In order to demonstrate the applicability of Patronus, we

978-0-7695-4944-6/12 $26.00 © 2012 IEEE
DOI 10.1109/SOSE.2013.14

implemented a prototype application for photo sharing on Android.

The rest of this paper is organized as follows. We present the background information and our motivation in Section I. The Patronus model is described in Section II. In Section III, we present the design and implementation of the prototype application for photo publication on Android. Case studies are provided in Section IV. Related works are reviewed in Section V. Finally, we conclude our work in Section VI.

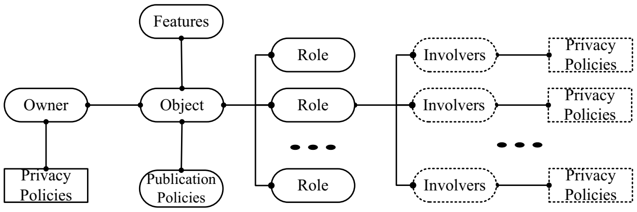


Figure 1. The Patronus Model

II. The Patronus Model

As we have demonstrated in Section I, it is far from enough to protect the privacy of users for resource publication in on-line social networks by employing the simple group-based access control model. In this paper, we introduce the concept of resource involvers, design a new format of privacy policies for users to specify their privacy requirements, and propose the Patronus model for resource publication in on-line social networks as shown in Figure 1.

A. Object and Features

The *object* refers to a certain resource, which is going to be published over on-line social networks. It can be a text message, an image, a video or a mixture of the above three. For example, an album, which is shared over on-line social networks, might include tens of images and several short descriptions; And there might be several photos or even videos as supporting materials in a blog, in addition to the body of the text.

The *Feature* describe the type of the object and the content of the object. There are four types in the Patronus model, including **TXT**, **IMG**, **VDO** and **MIX**. The contents of each object can be extracted and summarized with four key words, which are **WHEN**, **WHERE**, **WHO**, and **WHAT**.

Take a photo as an example. Its type should be set as **IMG**. And it contains the following content:

- **WHEN**: the time when this photo was taken
- **WHERE**: the place where this photo was shot
- **WHO**: the persons in the photo
- **WHAT**: what the persons are doing(e.g. drinking, swimming, running, working, playing and so on)

The features of Alice's photo in our motivating scenario can be represented as in Figure 2.

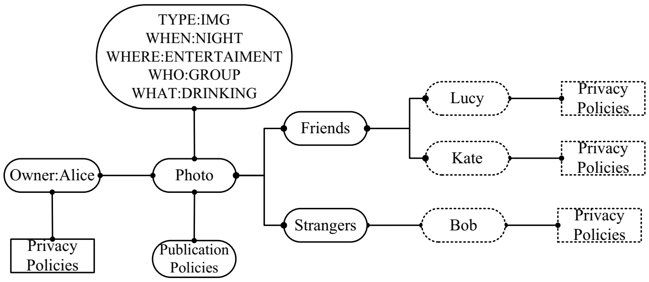


Figure 2. The Patronus Model Instance for the Motivating Scenario

B. Subjects

1) Owner: In the Patronus model, the owner refers to the user who has control during the publication of the object, instead of the original creator of the object. For example, a wedding video might be recorded by a professional photographer, and then released by the bride over on-line social networks to enjoy together with her friends. In this case, the photographer is the original generator of the video, but the bride is the owner of the video in our definition.

2) Roles and Involvers: The involvers of an object refer to the persons whose names are mentioned in the body of the text, or whose faces can be detected and recognized in the image/video. They are classified into different categories, and linked with the object in different roles.

As in our motivating scenario, the involvers of the photo are Lucy, Kate, and Bob. They are classified into two categories: Friends and Strangers. Lucy and Kate are Friends, and Bob is a stranger, as shown in Figure 2.

C. Policies

There are two kinds of policies in our Patronus model, including privacy policies and publication policies. Publication policies are calculated and generated with corresponding privacy policies, which indicate available on-line social networks and proper access control lists. And privacy policies are used to express the privacy preferences of the owner/involvers for social data publication, which include the following aspects:

- What kinds of social data are allowed to be published online?
- What kinds of social data should be blocked?
- Which on-line social networks are preferred?
- Which on-line social networks should be avoided?
- What kinds of access control lists should be set? Private, Public, or can only be accessed by a certain crowd, such as classmates, co-workers, friends, 2-degree friends and so on?
- Do they intend to protect the privacy of all the involvers, or just their friends, close friends, or even none of them?

In order to express the above information clearly and regularly, and make further calculation and evaluation easier, privacy policies are formatted as follows:

- $POLICIES \rightarrow kindness!policies$
- $kindness \rightarrow$ NONE | CLOSEFRIENDS | FRIENDS | ALL
- $policies \rightarrow policy; policies | \varepsilon$
- $policy \rightarrow to : \{rules\}$
- $to \rightarrow$ TWITER | PICASA | FACEBOOK
- $rules \rightarrow item, rules | \varepsilon$
- $item \rightarrow < lable : value >$
- $label \rightarrow$ TYPE | TXT | IMG | VDO | MIX |
  WHEN | DAY | NIGHT |
  WHERE | HOME | OFFICE | ENTERTAINMENT |
  WHO | SINGLE | GROUP |
  WHAT | DRINGKING | CRYING | OTHERS
  LEVEL | PRIVATE | PUBLIC | FRIENDS
- $value \rightarrow$ ON | OFF | $\{rules\}$

The following is a simple policy instance:

```
FRIENDS!

TWITTER:
{
  <TYPE:{<IMG:OFF>,<VDO:OFF>,<MIX:OFF>}>},
  <LEVEL:{<PUBLIC:ON>}>
};
PICASA:
{
  <TYPE:{<TXT:OFF>,<VDO:OFF>,<MIX:OFF>}>,
  <LEVEL:{<PUBLIC:OFF>,<FRIENDS:OFF>,<PRIVATE:ON>}>
};
FACEBOOK:
{
  <TYPE:{<VDO:OFF>,<MIX:OFF>}>,
  <WHEN:{<NIGHT:OFF>}>,
  <WHERE:{<HOME:OFF>,<OFFICE:OFF>}>,
  <WHO:{<SINGLE:OFF>}>,
  <WHAT:{<DRINKING:OFF>,<CRYING:OFF>}>
  <LEVEL:{<PUBLIC:OFF>,<FRIENDS:ON>}>
};
```

which indicates that:

- As the owner of an object, he/she only wishes to protect the privacy of his/her friends among the involvers who are related with her object;
- While as an involver of an object, she declares that only text messages are allowed to be published on the website of Twitter, and the corresponding access control lists are recommended as public;
- Only photos are agreed to be published on Picasa, and the corresponding access control lists should be set as private;
- On the website of Facebook, both text messages and photos can be shared with friends, however the following requirements should be satisfied simultaneously:
  - It didn't happen at night.
  - It didn't happen at home or in the office.
  - The subject is not the only one who involves with the object.
  - The subject was not drinking or crying.

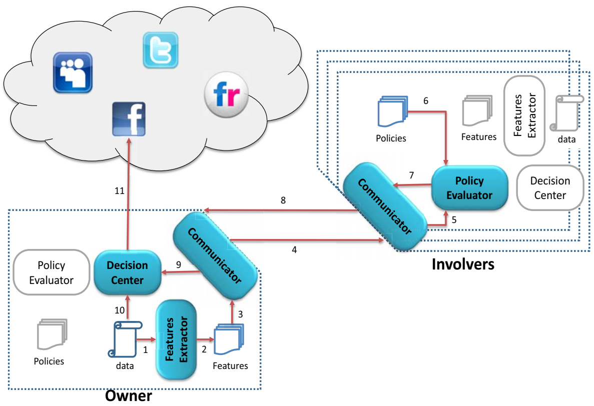


Figure 3. The Prototype Implementation of Patronus on Android

III. Prototype Design and Implementation

In the mobile computing world with various mobile devices such as smartphones and tablets, it is becoming much more convenient for individuals to generate various kinds of resources, and share them with their friends over on-line social networks.

As smart phones can be expected to become the major platform for resource publication in the near future, we choose the Android platform to implement a prototype based on Patronus for photo publication. The prototype runs on HTC Magic smartphones with Android 2.3 platform, with the MSM7200A 528MHz processor, 288MB RAM and 512MB ROM. The implementation of the prototype is shown in Figure 3.

A typical process in the prototype works as follows: As soon as a photo is taken, its features are extracted and stored locally. The corresponding involvers are then identified. When the photo is intended to be published online, its features are transferred to the involvers for privacy violation detection. The publication process will succeed if all permissions from the involvers are collected; otherwise, the process will be terminated automatically and the owner will be notified with a privacy violation warning.

A. Feature Extractor

As indicated in Section II, there are five essential features associated with a specific piece of social data, which are **TYPE**, **WHEN**, **WHERE**, **WHO**, and **WHAT**. The **TYPE** of the object is fixed as **IMG** in our prototype for privacy-preserving photo publication. The other four features are gathered by the Feature Extractor.

WHEN: It indicates the time information at which the photo is taken. Corresponding to the two terminals in our Patronus model, **DAY** and **NIGHT**, we define the time interval from 8:00 AM to 9:00 PM as **DAY**, and the opposite time interval from 9:00 PM to 8:00 AM as **NIGHT**.

WHERE: It indicates the location information at which the photo is taken. With the build-in GPS modular on smartphones, latitude and longitude information can be collected. We extracted the corresponding information from the *exif* part of a JPG photo[1].

WHO: In the Patronus model, there are two corresponding labels with the WHO feature: **SINGLE** and **GROUP**. The values of these two labels can be simply defined based on the results of face detection. Moreover, face recognition should also be applied in order to identify the corresponding involvers for further use.

WHAT: In the Patronus model, it is attached to two labels: **DRINKING** and **CRYING**. There are also some other events, such as running, jumping, swimming, singing, dancing, working, playing and so on. Additional labels can be added if necessary. But in our prototype, we assume that one might not wish photos, in which he or she is drinking or crying, to be published over on-line social networks, thus these two labels are enough. The value of **WHAT** is provided by the user manually.

The privacy policies of the user are also collected:

TO: It indicates which on-line social networks are preferred for the user. In the Patronus model, there are three corresponding labels: **FACEBOOK**, **PICASA** and **TWITTER**. Users can choose them according to their preferences.

LEVEL: It indicates the access control lists which will be set if the photo is published on a certain on-line social network. In the Patronus model, there are three corresponding labels, **PRIVATE**, **PUBLIC** and **FRIENDS**. Users can turn on/off different levels in their policies.

By employing the underlying services of the system time and GPS, the values of **WHEN** and **WHERE** can be generated, respectively. The values of **WHAT** and **TO** are set by the photo owner manually. According to the values of **TO**, the corresponding value of **LEVEL** are retrieved from the policies predefined by the user. The OpenCV tool for Android is employed for the **WHO**-values generation and involvers identification.

B. Communicator, Policy Evaluator, and Decision Center

As a deamon activity, the Communicator provides the following three functions: Features Sending and Receiving, Policies Sending and Receiving, and Responds Collecting. In our current implementation, features and policies are transferred in text messages. There is a keyword **PATRONUS** at the beginning of messages automatically generated by the prototype. So that, messages can be filtered and redirected to the Communicator without disturbing the user.

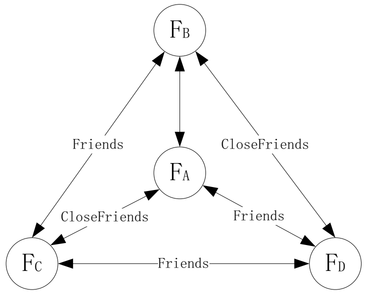


Figure 4. The Social Relationship Graph

The Policy Evaluator calculates the feature information received from the Communicator, and the decision center detects for violations with the calculated result and generate publication policies, which indicates whether or not a certain photo is allowed to be published on the line. Better choices of on-line social networks and the corresponding privacy level are suggested at the same time.

IV. Case Studies

We use 8 persons in our experiment. We assume that four of them are familiar with each other, whose head icons have already been pre-stored on their smartphones. The other four persons are considered as **Strangers**. The **Familiars** are indexed as F_A, F_B, F_C, and F_D. The social relationship between them is shown in Figure 4. And the **Strangers** are indexed as S_A, S_B, S_C, and S_D.

We prepared a 300-contacts address book for each person in our experiment. Only one-third contacts are edited with head icons. And among these 100 contacts, half of them are marked as Friends. A half of those friends are declared as CloseFriends.

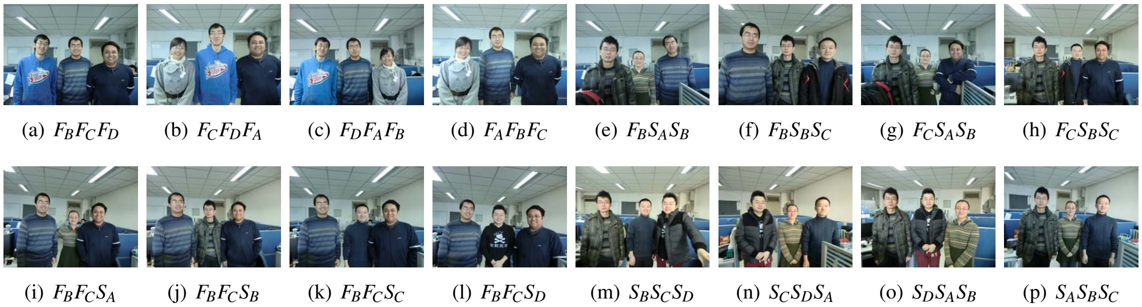
We prepared 16 photos, which can be classified into four categories: With no strangers in the photo, with only one stranger in the photo, with two strangers in the photo, and with no familiars in the photo. The photos are shown in Figure 5.

A. Privacy Policies of the Familiars

As the owner of an object, F_A would like to protect the privacy of all the involvers who are related with his/her object; And as an involver of an object, F_A declares that only photos, which were not taken at night, can be published on the social networks, including Twitter, Picasa and Facebook. Photos, which were posted on Twitter or Picasa can be shared with any one, but photos on Facebook can only be shared with friends.

As the owner of an object, F_B would like to protect the privacy of his/her friends who are related with his/her object; As an involver of an object, F_B declares that only photos, which were not taken in the office, can be published on

[1] For privacy concerns, location service is usually recommended to be turned off so that no location information can be associated with the photos taken by digital cameras or smart phones. However, only the privacy of the resource owner is considered and respected in such circumstances. In our prototype, since the location information of a photo is very important for involvers to determine whether or not the corresponding photo should be blocked, we turn on the location service by default.



(a) $F_B F_C F_D$ (b) $F_C F_D F_A$ (c) $F_D F_A F_B$ (d) $F_A F_B F_C$ (e) $F_B S_A S_B$ (f) $F_B S_B S_C$ (g) $F_C S_A S_B$ (h) $F_C S_B S_C$

(i) $F_B F_C S_A$ (j) $F_B F_C S_B$ (k) $F_B F_C S_C$ (l) $F_B F_C S_D$ (m) $S_B S_C S_D$ (n) $S_C S_D S_A$ (o) $S_D S_A S_B$ (p) $S_A S_B S_C$

Figure 5. Sample Photos

the social networks, including Twitter, Picasa and Facebook. Photos, which were posted on Picasa can be shared with any one, but photos on Twitter and Facebook can only be shared with friends.

As the owner of an object, F_C would like to protect the privacy of his/her close friends who are related with his/her object; As an involver of an object, F_C declares that only group photos can be published on the social networks, including Twitter, Picasa and Facebook. And photos can only be shared with friends instead of any one in the public.

As the owner of an object, F_D would not like to protect the privacy of the involvers who are related with his/her object; As an involver of an object, F_D declares that only photos, in which he/she was not crying, can be shared with any one in the public on the following social networks, including Twitter, Picasa and Facebook.

B. Cases

Figure 5(a)$\sim$ 5(d) are taken by F_A, F_B, F_C, and F_D respectively in this case. We suppose that the corresponding owner decides to publish the photo on the Facebook website. As shown in Tabel I, the ideal column shows the best results if the privacy of all involvers are respected. The expectation column shows the desired results with current policies. And the publication column shows the actual results in the experiments.

Table I
RESULTS FOR CASE #01

	F_A	F_B	F_C	F_D	Ideal	Expectation	Publication
F_A	-	$\surd$	$\surd$	$\surd$	Denied	Denied	Denied
F_B	$\times$	-	$\surd$	$\surd$	Granted	Granted	Granted
F_C	$\surd$	$\times$	-	$\times$	Denied	Granted	Granted
F_D	$\times$	$\times$	$\times$	-	Denied	Granted	Granted

Figure 5(e)$\sim$ 5(h) are taken by F_A and F_D in this Case. And both of them decided to publish these photos on the Picasa. As shown in Table II, the first four publications are all denied, because the photos which were taken in the office does not allowed to be published by F_B; and there are conflicts on the private policies of Picasa between F_A and F_C. The latter four publications are all granted because F_D does not wish to protect the privacy of anyone else as described in his policies.

Table II
RESULTS FOR CASE #02

	F_B	F_C	S_A	S_B	S_C	S_D	Expectation	Publication
F_A	$\surd$	$\surd$	$\times$	-	-	-	Denied	Denied
F_A	$\surd$	$\times$	-	$\times$	-	-	Denied	Denied
F_A	$\surd$	$\surd$	-	-	$\times$	-	Denied	Denied
F_A	$\times$	$\surd$	-	-	-	$\times$	Denied	Denied
F_D	$\times$	$\times$	$\times$	-	-	-	Granted	Granted
F_D	$\times$	$\times$	-	$\times$	-	-	Granted	Granted
F_D	$\times$	$\times$	-	-	$\times$	-	Granted	Granted
F_D	$\times$	$\times$	-	-	-	$\times$	Granted	Granted

Figure 5(i)$\sim$ 5(l) are taken by F_A, F_B and $F_C$in this case. And we also suppose the corresponding owner decides to publish these photos on the Facebook this time. As shown in Table III, the first two publications are denied because F_B disallow his photos which are taken in the office to be published. And the two publications of line 3 and 4 are granted just as F_C wishes. The two publications of line 5 and 6 are also granted because F_C only cares the privacy of his close friends. And the last two publications are granted because no privacy violations are detected.

Table III
RESULTS FOR CASE #03

	F_B	F_C	S_A	S_B	S_C	Expectation	Publication
F_A	$\surd$	-	$\times$	$\times$	-	Denied	Denied
F_A	$\surd$	-	-	$\times$	$\times$	Denied	Denied
F_A	-	$\surd$	$\times$	$\times$	-	Granted	Granted
F_A	-	$\surd$	-	$\times$	$\times$	Granted	Granted
F_C	$\times$	-	$\times$	$\times$	-	Granted	Granted
F_C	$\times$	-	-	$\times$	$\times$	Granted	Granted
F_B	-	$\surd$	$\times$	$\times$	-	Granted	Granted
F_B	-	$\surd$	-	$\times$	$\times$	Granted	Granted

Figure 5(m)$\sim$ 5(p) are taken by F_A, F_B, F_C, and F_D in this case. And this time the corresponding owner decides to publish these photos on Picasa. Since no familiars can be detected in these photos, the publications are all granted.

V. Related Work

In this section, we describe the work related to Patronus and its prototype implementation.

Privacy in on-line social networks has emerged as a hot topic for researchers and a serious concern for individual users. Although personal information is contained in both profiles and resources in on-line social networks, traditional privacy researches are mainly focused on protecting the sensitive information in personal profiles from adversaries.

As demonstrated in [1], current privacy settings in on-line social networks are too complicated for average users to handle, and too time-consuming for advanced users to configure. In order to release users from the heavy burden of privacy configuration, several assistant tools are developed [2] [3]. Tools are also developed to evaluate the current privacy settings of a certain user [4] [5]. In [6], new access control models, which are required in on-line social networks, are proposed and formalized. Access control policies are expressed as constraints on the type, depth, and trust level of existing relationships to enforce resource exchange across multiple social networks.

The OpenCV(Open Source Computer Vision Library) is a library of programming functions, which is widely used for object identification, face detection and recognition, motion tracking and understanding, gesture recognition and so on. In our prototype, the OpenCV 2.3.1 for Android, which was released on Aug. 12th, 2011, is employed for the identification of photo involvers[7], [8], [9].

TagSense[10] introduce an interesting method for image tagging with the help of smart phones.Taking advantages of the embedded sensors, information about the people and their activities can be collected. TagSense merged these information carefully together to create tags on-the-fly in the form of ”Who-What-Where-When”. The design of features in our Patronus model is motivated by TagSense.

In our Patronus model, the privacy policies associated with the subject are evaluated according to the features of the corresponding object, which is very similar to the existing context-aware/context-dependent privacy policies. By sensing and collecting information from the surroundings, users can define a variety of situations, and corresponding privacy policies should be selected and applied in a specific situation. As the changing of the situations, different actions can be performed accordingly[11], [12], [13].

VI. Conclusion

With the popularity of on-line social networks and the widespread of smartphones, more and more data containing personal information are published over the Internet every day, which might be lead to a serious privacy leakage. In this paper, we introduced the concept of **involvers**, and proposes a new access control model named Patronus for privacy-preserving data publication for online social networks. We assume that the individuals involved **intend** to protect the privacy of their friends whenever possible if asked. We implemented a corresponding prototype for privacy preserving photo sharing on the Android platform and demonstrated its applicability and practicality.

Acknowledgement

This work is supported in part by the National 863 Program under Grant No. 2011AA01A202, the NSFC under Grant No. 61103026, the NSFC/RGC Joint Research Project (No.60931160444), and a State Key Laboratory of Computer Architecture (ICTCAS) Open Project under Grant No. ICT-ARCH201009.

References

[1] R. Gross and A. Acquisti, “Information revelation and privacy in online social networks,” in *WPES ’05*, New York, NY, USA, 2005, pp. 71–80.

[2] G. Danezis, “Inferring privacy policies for social networking services,” in *AISec ’09*, New York, NY, USA, 2009, pp. 5–10.

[3] L. Fang and K. LeFevre, “Privacy wizards for social networking sites,” in *WWW ’10*, New York, NY, USA, 2010, pp. 351–360.

[4] H. R. Lipford, A. Besmer, and J. Watson, “Understanding privacy settings in facebook with an audience view,” in *UPSEC’08*, Berkeley, CA, USA, 2008, pp. 2:1–2:8.

[5] K. Liu and E. Terzi, “A framework for computing the privacy scores of users in online social networks,” *ACM Trans. Knowl. Discov. Data*, vol. 5, no. 1, pp. 6:1–6:30, Dec. 2010.

[6] B. Carminati, E. Ferrari, and A. Perego, “Rule-based access control for social networks,” in *OTM 2006 Workshops*. Springer Berlin Heidelberg, 2006, pp. 1734–1744.

[7] “OpenCV Android,” http://opencv.willowgarage.com/wiki/Android.

[8] “OpenCV Android Experimental,” http://opencv.willowgarage.com/wiki/AndroidExperimental.

[9] “Android CMake Dev Guide,” http://android-cmake.googlecode.com/hg/documentation.html.

[10] C. Qin, X. Bao, R. R. Choudhury, and S. Nelakuditi, “TagSense: A Smartphone-based Approach to Automatic Image Tagging,” in *MobiSys*, 2011, pp. 1–14.

[11] A. Behrooz and A. Devlic, “A Context-aware Privacy Policy Language for Controlling Access to Context Information of Mobile Users,” in *MobiSec*, 2011.

[12] R. Hull, B. Kumar, D. F. Lieuwen, P. F. Patel-Schneider, A. Sahuguet, S. Varadarajan, and A. Vyas, “Enabling Context-Aware and Privacy-Conscious User Data Sharing,” in *Mobile Data Management*, 2004, pp. 187–198.

[13] A. Corradi, R. Montanari, and D. Tibaldi, “Context-Based Access Control Management in Ubiquitous Environments,” in *NCA*, 2004, pp. 253–260.