Analysis of Access Control Mechanisms for Users’ Check-ins in Location-Based Social Network Systems

Lei Jin, Xuélian Long, James B.D. Joshi, Mohd Anwar
LERSAIS Lab, School of Information Sciences, University of Pittsburgh
Pittsburgh, PA, USA
{lej17, xul10, jjoshi, manwar}@pitt.edu

Abstract—Location-Based Social Network Systems (LBSNs) are becoming increasingly popular. In LBSNs, users can check in at various places, connect with their friends and share their check-ins (including users’ locations and timestamps) with their friends and even the public. However, most LBSNs pay more attention to attracting users to join and actively use their systems rather than protecting users’ privacy preferences for their check-ins. In this paper, we analyze access control mechanisms for users’ check-ins in four of the most popular existing LBSNs: Facebook Places, Foursquare, Google Latitude and Yelp. We first generalize a model for users’ check-ins based on these LBSNs. Considering users’ check-ins as the protection objects, we then generalize an access control policy model for them. We use these two models as criteria to analyze these access control mechanisms for users’ check-ins and compare them in these LBSNs. Additionally, we identify the common vulnerabilities in these access control mechanisms. Understanding the access control mechanisms for users’ check-ins and their limitations can help users who care more about their privacy to choose a LBSN where their location privacy is better protected.

I. INTRODUCTION

The increasingly widespread use of the smart phones (e.g. iPhones and Android Phones) with embedded GPS modules has significantly promoted the location-based social network systems (LBSNs). Most LBSNs have a check-in feature, which allows a user to explore various places around his current location. Users can check in at various places (publish his locations), and leave comments or tips about the places. In addition, similar to traditional social network systems (e.g. Facebook and LinkedIn), a user in a LBSN can add friends and share his check-ins that contain the user’s location information, with his friends. A user may share his check-ins with others in order to let more people know about his interests and to attract more to connect to him as friends to promote his popularity in the LBSN.

Although the benefits from LBSNs encourage a user to share his location, location privacy is a primary concern. The exposure of a user’s location information may bring unexpected troubles to the user. For example, Puttaswamy et al. [7] mention several reports of incidents where the exposure of a user’s locations have caused serious economical, social and physical concerns to the users; e.g., the exposure of a user’s visits to hospitals, nightclubs, or other locations could have social or physical consequences to users. A report from Yahoo described four types of crimes that result from a victim’s incautious broadcasting of his check-ins in Foursquare [6], such as home invasions (because of a check-in indicating a victim is not at home) and muggings (because of a check-in letting muggers know the exact location to rob a victim at).

LBSNs with the check-in feature typically also have the access control mechanisms that can be applied by a user to control the access to his check-ins. However, most LBSNs pay more attention to attracting users to join and actively use their systems rather than protecting their location privacy. There are a number of vulnerabilities in the access control mechanisms for users’ check-ins in LBSNs and these vulnerabilities can easily cause the exposures of users’ location information without users’ authorizations. For instance, a report in CNET presented a user privacy attack because of the absence of a policy mediation mechanism between Foursquare and Twitter [15]. In this attack, an attacker scraped data from public tweets, which had been pushed by Foursquare users from Foursquare and included the information of users’ check-ins. The attacker then built a website, called “Please Rob Me”, where he listed people who were currently not at home. The crux of this attack is that a user’s access control policies for his check-ins in Foursquare are not enforced in Twitter.

Users are becoming more concerned about their private information in online social network systems (OSNs) [8]. A LBSN is a type of OSNs and users’ locations in the LBSN are users’ sensitive information. Therefore, users should be aware of the vulnerabilities in the access control mechanisms for their check-ins in LBSNs that could cause the exposure of their location information. Users should be notified whether or not LBSNs can protect their specific location privacy preferences. They also have to know how to protect their location privacy in the LBSNs. In this paper, we focus on four of the most popular LBSNs which have the check-in feature: Facebook Place, Foursquare, Google Latitude and Yelp. We first analyze these LBSNs, and generalize a model of a user’s check-in and a model of an access control policy for a check-in. Then, we analyze the access control mechanisms in these LBSNs using these two models and make comparisons among them. Furthermore, we discuss the common vulnerabilities of these access control mechanisms. Our analysis would help a user to choose a LBSN which can support his privacy preferences. It can also help operators of a LBSN to design better privacy-protecting solutions. Our main contributions are as follows:
We generalize a user’s check-in model and an access control policy model for a check-in from four of the most popular LBSNSs. We regard these two models as criteria to analyze access control mechanisms for users’ check-ins in these LBSNSs and compare them.

We identify several common vulnerabilities regarding users’ check-ins in these four LBSNSs.

The rest of the paper is organized as follows. In Section 2, we present these LBSNSs and our analysis methodology. In Section 3, we analyze the access control mechanisms for users’ check-ins in these LBSNSs and make comparisons; we present the common vulnerabilities in the access control mechanisms used by these LBSNSs in Section 4. Finally, we discuss the related work in Section 5 and conclude with a discussion of future work in Section 6.

II. LBSNS SELECTIONS AND ANALYSIS METHODOLOGY

A. LBSNSs Selections

In this paper, as mentioned earlier, our focus of analysis is the four of the most popular LBSNSs, which are Facebook Place, Google Latitude, Foursquare and Yelp.

Facebook is the most popular traditional social network. Until March 2012, it had 901 million active users [1]. Facebook Place is one of Facebook features that allow a user to share his check-ins with other users in Facebook. Regarding the number of users who use Facebook Place, a survey shows that 44% of teenagers in United Kingdom are aware of Facebook Place and 30% of them have used it [2].

Google Latitude is another popular LBSNS. It allows users to share their check-ins with their contacts in Google (e.g., their friends in Google Plus) and the other users. A report from TechCrunch shows that there are 3 million active users in Google Latitude [3].

Foursquare is an application that allows a user to post his location as a check-in to the public or share it with his friends in Foursquare. A report estimated that Foursquare has 20 million users [4].

Yelp is another application that allows a user to check in at various places and to provide/share reviews for the places. A user in Yelp can also share his check-ins with his friends in Yelp. Yelp Press reports that Yelp has 71 million users [5].

B. Analysis Methodology

In Facebook Place, Google Latitude, Foursquare and Yelp, we first analyze the features in their check-in mechanisms by exploring their mobile applications in Apple iOS and Google Android. Since some access control policies can be set in the mobile applications and others have to be set in the web systems of these LBSNSs, we then analyze the privacy setting policies for a user’s check-in in the mobile applications as well as the web systems.

Based on our analysis, we first specify a check-in model that represents the protection object in these LBSNSs. We also extract an access control model for a check-in in order to generalize the access control mechanisms for users’ check-ins in these LBSNSs. We use these two models as criteria to analyze access control mechanisms for users’ check-ins in these LBSNSs and make comparisons among them.

III. ACCESS CONTROL MECHANISMS OF USERS’ CHECK-INS IN LBSNSs

A. Models in a LBSNS

Inspiring by [11], we represent a LBSNS as \( G(V, E, C, T) \) where \( V \) represents the user set, \( E \subseteq V \times V \) is a set of relationships between users, \( C \) is users’ check-in set and \( T: V \rightarrow C \) is a function that assigns check-ins to users.

In addition, a user \( u \in V \) has a check-in set \( C_u \subseteq C \) which represents all of \( u \)'s check-in records in a LBSNS. Based on our analysis in Facebook Place, Google Latitude, Foursquare and Yelp, a check-in \( c \in C_u \) has four types of the resources \((l, t, OU, M)\) and hence can be modeled as a five tuple \(<u, l, t, OU, M>\) where

- \( u \) represents the creator and the owner of \( c \).
- \( l \) represents the location information of a place.
- \( t \) represents the timestamp indicating when \( c \) occurs.
- \( OU \) represents other users that \( u \) is with when he creates \( c \).
- \( M \) represents messages (comments or tips) that are associated with \( c \).

Example 1: assume a user \( u_1 \) checked in at LERSAIS Lab, School of Information Sciences, University of Pittsburgh with \( u_2 \) and \( u_3 \) at 10am on Apr. 30 of 2012 and posted a message \( m \) “\( u_1, u_2 \) and \( u_3 \) is having a group meeting now” in Facebook Place. This check-in can be presented as \( c = <u_1, \text{LERSAIS Lab, School of Information Sciences, University of Pittsburgh}, \text{2012-04-30 10:00:00}, \{u_2, u_3\}, \text{"having a group meeting now"}>.\)

In a LBSNS, \( l, t, OU, M \) in a check-in \( c \) are the objects a user \( u \) expects to be protected. This is because these resources contain \( u \)'s private information. In a check-in \( c \), \( l \) can represent the sensitive information, such as \( u \)'s home address. \( t \) is also the private information that could be risky for \( u \) in some scenarios. For instance, a house robber may be very interested to know the time when \( u \) is not at home. \( OU \) is usually sensitive, especially when \( u \) checks in at a place with other users. These users may not allow \( u \) to share their locations with the people who are not their friends. In addition, messages (e.g., private comments) in \( M \) in \( c \) may contain sensitive information that \( u \) may not want to share with all the users.

Generally, a user \( u \) needs a policy \( P_u \) to control access to \( C_u \) in a LBSNS. In addition, for each \( c \in C_u \), there is a set \( P_{uc} \subseteq P_u \) that represents policies for \( c \). Our analysis of the access control policies in these four LBSNSs reflects that a policy statement \( p \in P_{uc} \) can be modeled as six tuple \(<r, S, U, a, d, r>\) where

- \( c \) is a five tuple \(<u, l, t, OU, M>\) and represents \( u \)'s check-in record in \( C_u \), as discussed earlier. It indicates the entities that need to be protected by a policy.
• $S$ is a system set (including LBSNSs and other social network systems) and represents where $c$ is created and/or posted.

• $U$ is a user set and specifies users for whom $p$ applies in the specified $S$. Note that $U$ cannot contain the users who are not in any system in $S$.

• $a$ represents an action for $c$. The action can be “create”, “modify”, “delete” and “read”. For instance, when a user has “delete” privilege on $c$, he can delete $c$.

• $d$ represents the available duration of $c$ for users in the $U$ in $S$. After the duration, $c$ will no longer be available for them.

• $r$ represents the access decision made by $u$ for $c$. The decision can be “allow” or “deny”.

Example 2: Assume a user $u$ has a check-in $c$ in Foursquare and he has the following settings: 1) $c$ is public to any user in Foursquare in two hours after it is created; 2) $c$ is posted to $u$’s Facebook account and it is public to his friends in Facebook with no limit on time. Such settings can be presented as follows:

- $p_1 = \ll ("Foursquare"), \ll "public", \ll "read", \ll "2 hours after it is created", \ll "allow" \gg$ where “public” represents any user in Foursquare.

- $p_2 = \ll ("Facebook"), \ll F_{pb}(u), \ll "read", \ll "without limit", \ll "allow" \gg$ where $F_{pb}(u)$ represents $u$’s friends in Facebook.

In the following, we analyze the access control mechanisms in Facebook Place, Google Latitude, Foursquare and Yelp using these two models.

B. Analysis of Access Control Mechanisms in LBSNSs

Table I lists the available resources in a check-in and Table II summarizes supported options in an access policy in in Facebook Place, Google Latitude, Foursquare and Yelp.

How the access control mechanism works

When a user $x$ requests an access to $c$ that belongs to a user $u$, the following access control mechanism steps occur in these LBSNSs:

1. The access control mechanism first identifies which system $x$ comes from and whether or not there is a policy for $x$ in $P_{au}$ in the system. When there is no policy, $x$’s request gets denied.

2. When there are several policies in $P_{au}$ that applies for $x$, the access control mechanism continues to identify whether or not $x$’s action and the current time satisfy the specified conditions in these policies. When these conditions are not satisfied, $x$’s request gets denied.

3. When the conditions in the policies are satisfied, the access control mechanism then identifies what are the access decisions of these policies. When all these decisions are “allow”, $x$’s request are allowed. Otherwise, $x$’s request are denied.

How to set & control a check-in $c$

In a check-in $c\ll u, l, t, O, M \gg$ created by a user $u$ in these four LBSNSs, $u$ has to choose a $l$ from a list of places, which are provided by LBSNSs based on the physical location captured by the GPS module embedded in the smart phone, to check in. In particular, $u$ in Google Latitude can manually set the geo-coordinates and check in there. $u$ cannot set $t$ in $c$ in all the four LBSNSs. The LBSNSs automatically acquire it. Regarding $OU$ in $c$, $OU$ is equal to $\ll u \gg$ in Google Latitude, Foursquare and Yelp. In Facebook Place, $u$ can check in with his friends. In this case, $OU$ can be the subset of the set including $u$ and $F(u)$ ($u$’s friends). In Facebook Place, Foursquare and Yelp, $u$ can create a message $m \in M$ associated with $c$ and other users can give comments for $m$. However, $u$ cannot do so in Google Latitude.

In these four LBSNSs, a check-in $c$ is modeled as an atomic resource. There is no fine-grained access control policy to control the access to the resources $l$, $t$, $OU$ and $M$ separately in $c$. Access to $l$, $t$, $OU$ and $M$ are either granted together or denied together.

How to set $S$ in an access policy $p$

In each of these four LBSNSs, a user $u$ can post his check-ins into the system at which the check-ins are created. In this case, $S$ contains only that system. For instance, a user can post his check-in into Facebook Place and hence $S=\ll "Facebook" \gg$.

In addition, $u$ can post his check-ins created in Foursquare or Yelp to Facebook and Twitter. Thus, in Foursquare, elements in $S$ could be a subset of $\ll "Foursquare", "Facebook", "Twitter" \gg$ while elements could be a subset of $\ll "Yelp", "Facebook", "Twitter" \gg$ in Yelp. $u$ can set $S$ when he is posting his check-ins.

Who can see a user’s check-in

In an access control policy $p\ll c, S, U, a, d, r, \gg$, a user $u$ usually has the following options for $U$ in a system $s \in S$:

- public: $u$ can share $c$ with the public. It means $c$ is public to any user in $s$.

- friends: $u$ can share $c$ with his friends in $s$.

- private: $u$ does not share $c$ with anyone in $s$.

In Facebook Place and Google Latitude, $u$ can set $U=\ll "public", "friends" \gg$ and $U=\ll "private" \gg$. In Yelp, $u$ cannot set $U=\ll "public" \gg$. Note that, according to the official explanation of “public” in Foursquare, $U=\ll "public" \gg$ means $c$ is shared with the people who are currently checked in at a place in $c$. In fact, any Foursquare user can obtain $c$ when he currently views the place’s profile page but not necessary checks in at the place.

In addition, since Facebook implements a fine-grained access control mechanism for a user’s posts and allows the user to group his friends, the user can share $c$ with specific friends and/or friend groups in Facebook Place when he sets $U=\ll "friends" \gg$. For instance, when a user is checking in at his home, he can set such a check-in only available for a specific group of his friends, e.g. the group named “Family”.

---

1 Please note that Facebook Place is a feature in Facebook.
How to set the duration of a check-in

A user can set the duration of a check-in by default in Google Latitude and Foursquare automatically check out a user at a place after he checked in at the place in $d$ (e.g., two hours in Facebook Place) and if he did not check in at another place during this period.

How to set the access decision of a check-in

In Google Latitude, Foursquare and Yelp, a user $u$ has only one option for $d$ in a policy $p(c, U, a, d, r)$, i.e., "allow". In Facebook Place, $u$ can set a $p$ either to be allowed or denied.

How to share a user’s check-in history $C_u$

In a LBSNS, a user $u$ can check in at various places and hence he has a check-in history $C_u$. In Facebook Place, when $u$ shares all check-ins with his friends, these friends can get all of $u$’s check-in records at any time. In Google Latitude and Yelp, $u$’s friends can only obtain $u$’s last check-in at a certain time although $u$ shares multiple of his check-ins to his friends. In Foursquare, $u$’s friends can only obtain $u$’s latest five check-ins at a certain time when they go through $u$’s profile page in the website of Foursquare. Specially, $u$’s friends in Foursquare can find the top visited places and the most explored venue categories where $u$ checked in in the last six months. For instance, assume the most explored venue category of a user $u$ is Bar in the last six months. Then, his friends can acquire $u$’s every check-ins that associate with Bar.

Table I. Available Features about Check-in in Facebook Place, Google Latitude, Foursquare and Yelp

<table>
<thead>
<tr>
<th></th>
<th>A User’s Check-in($c$)</th>
<th>Resources in a Check-in $c$</th>
<th>A User’s Check-in History ($C_u$)</th>
<th>A User’s Future Check-ins ($P-C_u$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook Place</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Google Latitude</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>*</td>
</tr>
<tr>
<td>Foursquare</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>#</td>
</tr>
<tr>
<td>Yelp</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>*</td>
</tr>
</tbody>
</table>

- ● means the feature is available; * means the last record in $C_u$; # means latest records in $C_u$

Table II. Access Control Policy for a User Check-in $c$ in Facebook Place, Google Latitude, Foursquare and Yelp

<table>
<thead>
<tr>
<th></th>
<th>Conditions and Result in an Access Control Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$S$</td>
</tr>
<tr>
<td>Facebook Place</td>
<td>Facebook</td>
</tr>
<tr>
<td>Google Latitude</td>
<td>Google Latitude</td>
</tr>
<tr>
<td>Foursquare</td>
<td>Foursquare; Facebook; Twitter; Public; Friends; Private; Create; Read;</td>
</tr>
<tr>
<td>Yelp</td>
<td>Yelp; Facebook; Twitter; Friends; Private; Create; Read;</td>
</tr>
</tbody>
</table>

What can a user do for a check-in

A user $u$ usually has the following options for $a$ in a $p(c, U, a, d, r)$ in LBSNSs:

- **Create**: All these four LBSNSs allow only $u$ to create his check-in $c$ in the system. In detail, $u$ can select $l$, define $O$ and add a message $m$ to $M$ in $c$.
- **Modify**: Google Latitude, Foursquare and Yelp do not allow any user to modify any created check-ins. In Facebook Place, $u$, the owner of $c$, can modify $c$. In addition, other users who are involved in $c$ can remove their identities in $c$ in Facebook Place.
- **Delete**: Only Facebook Place allows $u$ to delete his check-ins in Facebook.
- **Read**: All these four LBSNSs allow $u$ to read to $c$ in the system. $U$ can also define a $p$ that allows other users to read $c$.

How to set the duration of a check-in

In all these four LBSNSs, there is no option for a user $u$ to set $d$ in a $p(<, U, a, d, r)$ for his check-in $c$. In Facebook Place and Yelp, $u$ is assumed to be always at the place that associates with $c$ until he checks in at a different place. In Google Latitude, $d$ is set by default as a few days while $d$ in $c$ is set as two hours by default in Foursquare. In other words, Google Latitude and Foursquare automatically check out a user at a place after he checked in at the place in $d$ (e.g., two hours in Foursquare) and if he did not check in at another place during this period.
category Bar in the last six months, although these check-ins are not u’s last five check-ins.

**How to share a user’s future check-ins**

In Foursquare, a user u can have a “To-Dos List” (shown as $F-C_u$ in Table I) which shows the places u are very interested in and will check in at. This list is public to u’s friends and u cannot set any policy for this list. In Facebook Place, Google Latitude and Yelp, there is no feature like this.

**C. Comparisons among Access Control Mechanisms in LBSNSs**

According to Table I, we can see that Facebook Place supports the most features related to a user’s check-in. From Table II, we also find the Facebook Place has the most options for a user to set the access to his check-ins. It also implements the fine-grained access control mechanism for a user to share his check-ins to other specific users. Therefore, we believe that Facebook Place is more secure for a user to share his check-ins than the other three LBSNSs.

In Google Latitude, Foursquare and Yelp, a serious problem is that users can neither modify nor delete their check-ins. Another problem is that a user cannot share his check-ins with other specific users in these LBSNSs. Without such mechanism, a user’s privacy preference will be violated in some cases. For instance, assume a user adds his family members as friends in Foursquare. He is checking in with his friends at a night bar in midnight and he expects that this check-in is only available to his friends at the bar and it is not available to his family members who asked him to go asleep early. However, since Foursquare does not implement such a fine-grain access control mechanism, the user’s privacy preference is not satisfied.

**IV. DISCUSSIONS**

In this section, we discuss issues in these access control mechanisms that could cause privacy risks for users in these LBSNSs.

**No Access Control for Resources in a Check-in c**

We find that there is no a fine-grained access control mechanism for the resources l, t, $OU$ and $M$ separately in a check-in c in these four LBSNSs. Access to l, t, $OU$ and $M$ is either granted together or denied together. For instance, in Example 2, assume $u_1$ plans to share the location information (“LERSAIS Lab, School of Information Sciences, University of Pittsburgh”) in the check-in with the public. But he does not expect to expose the timestamp (“2012-04-30 10:00:00”) and the message (“having a group meeting”) to the public. In these four LBSNSs, $u_1$ cannot define a policy to control the access to the timestamp and the message that associates with c. Additionally, assume $u_1$ regards $u_2$ as his secret friend. He does not plan to tell the public he checked in with $u_2$ but he likes to tell the public he checked in with $u_2$. In these four LBSNSs, $u_1$ cannot have a policy to satisfy the requirement.

Without such a fine-grained access control mechanism for the resources in a user’s check-in, a LBSNS may bring many inconveniences and privacy risks for users in the LBSNS. Therefore, much fine-grained access control mechanisms are needed to allow users to control access to every resource in his check-ins.

**Other Users’ Controls for a Check-in Where these Users are Involved**

In Facebook Place, multiple users can be involved in a check-in. However, similar to the co-location privacy problem identified in [14], we find that a user $v \in OU$ in a check-in $c(l, t, OU, M)$ may unwillingly expose his location in c. For instance, $v$ may care more about his location information and he may not expect the users who are not his friends to obtain his location at a certain time. However, a user u who is a friend of $v$ can post a check-in with v to the public before obtaining v’s authorization in Facebook Place. Although v will be notified that he is involved in u’s check-in after the check-in is published and v can remove his identity in u’s check-in, other users can still identify v’s location from u’s check-in before v removes his identity in u’s check-in. Thus, v’s privacy preference is violated.

As a result, we believe that a policy negotiation mechanism among users should be developed and enforced in LBSNSs to solve the privacy risk discussed above. In such a policy negotiation mechanism, before a user u shares a check-in c that involves with other users, u should negotiate with these users and get their authorizations.

**Consistency of Access Control Policies Among Systems**

In Foursquare or Yelp, a user u can post his check-in created in Foursquare or Yelp to Facebook and Twitter. However, there is no policy mediation mechanism among these systems and it could cause privacy validations for a user’s location privacy.

For instance, assume that a check-in c is created by u in Foursquare and it is set to be available to u’s friends in Foursquare. When u posts c to Twitter as a tweet (assume that u’s tweets are set to be public), u’s privacy policy for c in Foursquare is violated. This is because the users who are not u’s friends in Foursquare have an opportunity to get c from u’s tweets when they identify u’s Twitter account. Additionally, in Foursquare, the duration of a check-in c is two hours. However, when c is posted to Twitter, c’s duration is changed. u’s friends who identify u’s location only from Twitter may believe that u was in the location in c for a much longer period till u posts the next check-in in Twitter.

Hence, the mediation mechanism to maintain the consistency of the access policies among systems should be implemented in order to better satisfy users’ privacy preferences.

**Other issues**

There is no setting for the available duration of a check-in in LBSNSs we analyzed. In other words, a user cannot set when his check-ins start to be available and when his check-ins are no longer made available to other users. The settings for the duration of a check-in could help a user to protect his privacy preferences in a better way. For instance, a user u is on vacation in a city which is far away from his home. He likes to check in at the places of interests in the city and shares these check-ins with users in Foursquare. However, he does not expect these check-ins are shared in Foursquare immediately when he is checking in at these places. He expects these check-
ins are shared when he comes back from the vacation in order to avoid a house theft. When a LBSNS has the settings for the available time of a check-in, u’s privacy preference can be achieved.

We also identify that a user’s actions and user’s decisions in an access control policy p(c, U, a, d, r) are limited in LBSNs. For instance, a user u cannot delete his check-ins in Google Latitude, Foursquare and Yelp. In these four LBSNs, u cannot modify c. In addition, u cannot set a “deny” policy in Google Latitude, Foursquare and Yelp which can introduce many inconveniences for users. For instance, assume a user u has hundreds of friends and he does not plan to share his check-ins at a night club with his girlfriend in Foursquare. To do so, u may need to manually add hundreds of his friends except his girlfriend to a new defined U in p. Such a task may cost a long time to finish. Therefore, we believe that LBSNs should support more actions and decisions in p in order to allow a user to manage his check-ins and set access control policies to the check-ins more conveniently.

V. RELATED WORK

As the first work of the large-scale quantitative analysis in a real-world LBSNS, Li and Chen analyze users’ profiles, activities, mobility characteristics, social graphs, and attribute correlations in Brightkite to identify relationships between physical locations and gain insights on users’ travel patterns [9].

Chen and Rahman analyze the privacy designs of 31 mobile social networking applications in the Apple iOS [10]. Their work focuses on what location information is collected and how it is used in these mobile applications. Compared to their work, our work aims to analyze the access control mechanisms for users’ check-ins.

Vicente et al. analyze the location-related privacy issues in Geo-social networks which include LBSNs [14]. Their work also identifies four types of privacy threats in Geo-social networks: location privacy (exposure of users’ locations), identity privacy (identifying users based on their locations), absence privacy (infer users’ absences at various locations) and co-location privacy (location exposure in the check-ins involving multiple users). Our work confirms that the problems from the absence privacy and the co-location privacy have not been addressed and they still exist in LBSNs.

Madejski et al. measure users’ sharing intentions in Facebook to identify violations in users’ privacy settings [12]. Their results indicate that every one of the 65 participants had at least one confirmed policy inconsistency. Their results confirm our argument - it is important to design a policy mediation mechanism for a user to share his check-in among multiple systems.

Kayastha et al. summarize the design architectures, content sharing protocols and the existing solutions for privacy issues in LBSNs [13]. Access control mechanisms for users’ check-ins in LBSNs may be improved based on these solutions.

VI. CONCLUSIONS

LBSNs are becoming increasingly popular and the benefits from LBSNs encourage a user to share his location information in LBSNs. However, the user’s location privacy is a primary concern. In this paper, we have analyzed access control mechanisms for users’ check-ins in four of the most popular LBSNs. We have first generalized a check-in model and a model of an access control policy for a check-in based on our analysis in these LBSNs. We have then used these two models as criteria to analyze access control mechanism for users’ check-ins and then compared them with each other. In addition, we have discussed the common vulnerabilities in these access control mechanisms. We believe that our analysis can help users to choose a LBSNS which is more consistent with his privacy preferences. As the future work, we plan to design a universal access control mechanism for users’ check-ins which does not have the vulnerabilities we discussed in the paper and can be applied in a real-world LBSN.

REFERENCES