International Journal of Computing Science and Information Technology, 2018
ISSN: 2278-9669,April 2018 (http://ijcsit.org)

The Privacy Issues With Third Party Applications On Facebook

Dr. N. Jayalakshmi[1].
Professor, Dept. of CSE,
Saveetha Engineering College, Chennai.

R.G. Kavitha[2].
Research Scholar,
Research & Development Centre,
Bharathiar University, Tamilnadu.

Received January 2018

Abstract

Facebook has become a potential target for the attackers due to the availability of sensitive information as well as its large user base. Therefore, privacy and security issues in Facebook are increasing. Privacy issue is one of the main concerns, since many Facebook users are not careful about what they expose on their profiles. Online interaction and sharing of personal information in Facebook has raised new privacy concerns. An additional dimension is added by the large amount of data collection and transmission by third-party applications on Facebook. This paper presents a privacy model to address users' privacy concerns toward third party apps on Facebook. This paper also presents a survey on different frameworks and improved interface designs which technically enforces the protection of the personal information of a user, when interacting with third party applications on Facebook.

Keywords: Privacy, Facebook, Third Party Applications, Privacy Model

1. Introduction

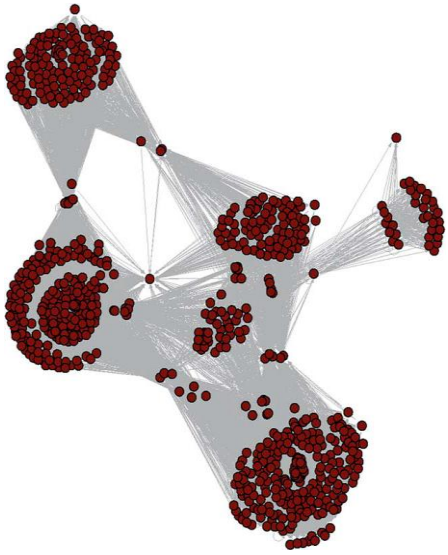
Facebook enables third-party developers to offer services to its users by means of Facebook applications. When a user adds a Facebook application to his profile, the user grants the application server to access a subset of the information listed on the user's Facebook profile and to perform certain actions on behalf of the user. Facebook grants these permissions to any application for each user who installs the application. Thereafter, the application can access the data and perform the explicitly permitted actions on behalf of the user.

Often, apps need certain types of data to function properly, but at other times, the apps do not need the unnecessary information to perform effectively, although the developers still request that extra information, according to the researchers, who released their findings on December 14 at the International Conference on Information Systems in Fort Worth, Texas. Pew Research Center survey found that apps are now asking for 235 different types of permissions. So apps are increasingly a confusing minefield of privacy issues. The aggressive way of data access and transmission by third party applications has raised the privacy concerns of the Facebook users. A privacy model for third party applications on Facebook is proposed in this paper to enhance the personal level privacy in Facebook. Different privacy frameworks and improved interface designs in Facebook to prevent from the privacy issues are also discussed in this paper.

2. Detecting Malicious Facebook Applications

Copyright © 2018 IJCSIT.

Sazzadur Rahman et. al developed FRAppE—Facebook's Rigorous Application Evaluator—arguably the first tool focused on detecting malicious apps on Facebook. It can detect malicious apps with 99.5% accuracy, with no false positives and a high true positive rate (95.9%). It used data from MyPage



++ -Keeper, a security app in Facebook that monitors the Facebook profiles of 2.2 million users. 111K apps that made 91 million posts over 9 months were also analyzed.

Figure 1. Emergence of app-nets on Facebook. Real snapshot of 770 highly collaborating apps: An edge between two apps means that one app helped the other propagate. Average degree (number of collaborations) is 195.

FRAppE—a malicious app detector that utilizes aggregation-based features in addition to the on-demand features. The on-demand features associated with an application refer to the features that one can obtain on demand given the application's ID. Such metrics include app name, description, category, company, and required permission set. Aggregation-based features for an app cannot be obtained on demand. These features are gathered by entities that monitor the posting behavior of several applications across users and across time.

Since the aggregation-based features for an app require a cross-user and cross-app view over time, FRAppE can be used by Facebook or by third-party security applications that protect a large population of users. It is also found that many apps collude and support each other; in the dataset, it is found that 1584 apps enabling the viral propagation of 3723 other apps through their posts. Figure 1 shows emergence of app-nets on Facebook [7].

3. Recognizing Malignant Facebook Application

Kiran Bhise et. al proposed system which can predict malicious application with better results as compared to an existing system. Malicious and benign apps datasets are input to the system. It implements the classification technique. It uses FRAppE (Facebook's Rigorous Application Evaluator) Classifier to identify the features of the apps. On demand features are calculated and aggregation is performed by using FRAppE.

Then the applications are analyzed with respect to aggregation based features. In this system, two new features are added like number of user ratings and user reviews to improve the accuracy of system and decrease false positive rate. Every app has few reviews as a feedback from the user side. All that reviews are considered for checking an app is malicious or benign. Figure 2 depicts an overview of the proposed system [8].

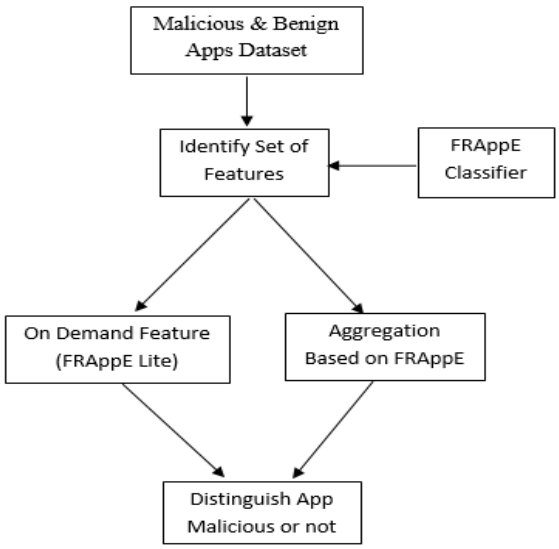


Figure 2: System Overview

4. OAUTH (Open Authorization) Framework

Mohamed Shehab et al. proposed OAuth framework. It provides a secure and efficient mechanism for authorizing third-party applications without releasing a user's access credentials. OAuth framework increases user privacy by separating the role of users from that of third party applications. Users need not share their private credentials with third party application, instead OAuth issues a new set of credentials. These new credentials are represented via an Access Token. An access token is a string which denotes a unique set of permissions

Copyright © 2018 IJCSIT.

granted to a third party application. After getting the approval from the resource owner, an authorization server issues access token to the third party application. Authorization code flow is shown in the figure 3. The authorization flow process consists of three parties: End-user (resource owner) at browser, Client (third-party application), Authorization server (e.g., Facebook). When a third party application needs to access user's resources, it presents its Access Token to the service provider. The authorization server authenticates the end user, and decides whether to grant or deny the third-party application's access request [1].

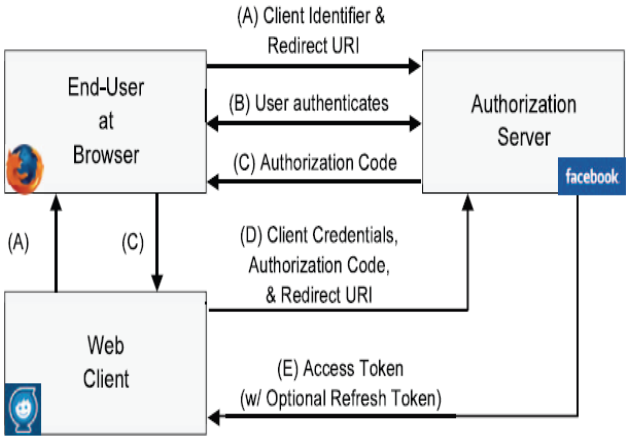


Figure 3. Authorization code OAuth flow

5. Footlights

Jonathan Anderson et al. designed and implemented an architecture called footlights. Footlight's design constraint is trust. Users need not trust any third party with their private data.

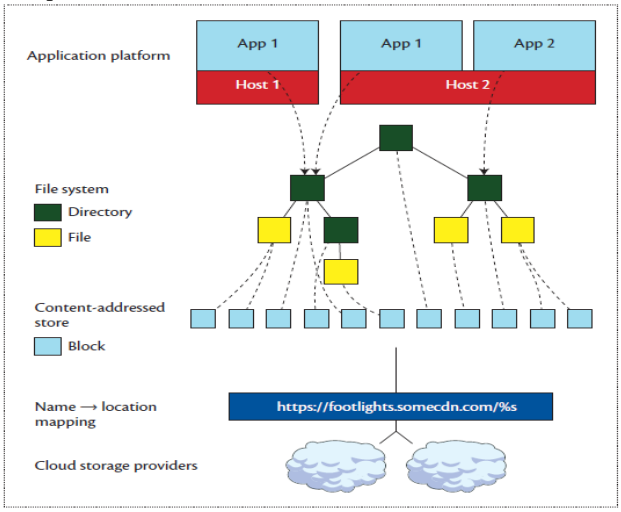


Figure 4. File system layers visible to applications.

Footlight uses cloud storage providers to hold user data. This data is broken into fixed sized blocks and then encrypted. When the users share with their friends, footlights reveals encryption keys to the client software of the chosen users only. The local Footlights client software interprets blocks that have been shared with it as a file system. The subsets of these data can be exposed to applications through a security API. Figure 4 shows file system layers visible to applications. Footlights provide an API that lets applications work with user data but not leak it beyond the user's consent.

Applications bundle files in a directory to be shared with other users, but footlights allows sharing only with explicit expression of user intent. Applications can access data such as photos directly if the user explicitly expresses intent [2].

6. Privacy Concerns Related to Facebook and Third-Party Applications.

Jennifer King et al. conducted a novel exploratory survey to measure how Facebook app users interact with apps, what they understand about how apps access and exchange their profile information, and how these factors relate to their privacy concerns. It is found that misunderstandings and confusion abound about how apps function and how they manage profile data. It also reveals that expectations, knowledge or behavior weren't consistent predictors of privacy concerns with third-party apps on SNSs in general. Instead, whether or not the respondent experienced an adverse privacy event on a SNS was a reliable predictor.

To explore these issues, an app was created and deployed it on Platform in order to conduct a non-random, exploratory survey (N=516) on how Facebook users perceive apps, what they know about them and the platform, and how these relate to their privacy concerns. It began with a review of descriptive statistics about app usage, comprehension, and privacy attitudes. Next, it explored the relationship between respondents' knowledge and behavior of third-party apps and their privacy attitudes in three areas: privacy-risky practices by third party apps, privacy concerns related to other users on Facebook, and privacy concerns related to the company itself. This survey says that over 90 percent of the respondents were very or somewhat uncomfortable with all of the three practices that were asked about: an app selling their profile information, storing the information permanently on its own servers, or sharing their data with other companies [6].

7. Access Control Framework for Third Party Applications

Mohamed Shehab et al. presented an access control framework to manage third party applications. This

framework is based on enabling the user to specify the data attributes to be shared with the application and at the same time be able to specify the degree of specificity of the shared attributes. This framework uses the required user profile attributes as conditions governing the application execution. This mechanism enables the application developer to select the data items required by the application and at the same time enables the user to opt-in or opt-out or generalize each of the requested data items. It is characterized by three main phases: application registration, to register the application at the social network server; user application addition, to add the application in a local profile; and application adaptation, within which the application adapts according to the provided data items.

An example of XML encoding for the horoscope application sheet is reported in the Figure 5(a), where birthday, gender and address are requested. In Figure 5(b), the user sheet is reported in which the user opted to disclose only day and month of birth[4].

a

```
<APPSHEET>
 <APP id="332198764">
  <DESCRIPTION>
   <NAME> Horoscope App </NAME>
   <INFO> Provide daily horoscope
    from www.horoscope.com </INFO>
  </DESCRIPTION>
  <DATA-GROUP>
   <DATA ref="birthday"/>
   <DATA ref="gender"/>
   <DATA ref="address"/>
  </DATA-GROUP>
 </APP>
</APPSHEET>
```

Application Sheet

b

```
<USERSHEET>
 <APP id="332198764">
  <ALLOW>
   <DATA-GROUP>
    <DATA ref="birthday.day"/>
    <DATA ref="birthday.month"/>
   </DATA-GROUP>
  </ALLOW>
 </APP>
</USERSHEET>
```

User Sheet

Figure 5 Application and user sheets.

8. The Development of New Designs for Authorization Dialogues

Na Wang et al. reported the results of an experimental study examining the limitations of current privacy authorization dialogues on Facebook as well as four new designs which were developed based on the Fair Information Practice Principles (FIPPs).

Facebook authorization dialogue for third-party apps are studied from different perspectives and several significant problems in information transmission are identified.

Problem 1: When an app is asking for publishing permissions and data access permissions at the same time, users are confused and may not be able to distinguish these permissions and do not know how the app will use their information.

Problem 2: During the process of adding an app to users' profiles, they do not have any control to limit or configure the app's access to their information or restrict app's publishing ability.

Problem 3: During the process of adding the apps to their profiles, users do not have any control to limit whether other users can see their app activities

Problem 4: Users may easily give out particularly sensitive private information or share information with third parties from which crucial identifying data can be inferred.

Based on the FIPPs, the following design principles are proposed:

Principle 1 (Notice/Awareness): The authorization dialogue should provide explicit information for users to learn what data would be accessed by the app and how the data would be used.

Principle 2 (Choice/Consent): The authorization dialogue should provide options for users to r profile (i.e., at installation time).

Principle 3 (Access/Participation): The authorization dialogue should provide options for users to control who can see their app activities.

Principle 4 (Notice/Awareness): The authorization dialogue should provide alert signals for users when the app asks for users' sensitive private information [9].

9. Privacy and the Illusion of Control

Na Wang et al. proposed the two new interface designs for third-party apps' authentication dialogs to: i) increase user control of apps' data access and restrict apps' publishing ability during the process of adding them to users' profiles, and ii) alert users when their global privacy settings on Facebook are violated by apps.

The following four design principles were proposed.

Known information – The authentication dialog should provide explicit signals for users to distinguish what data would be accessed by the app and how the data would be used.

Control before allowing – The authentication dialog should provide options for users to control the app's data reading and writing practices before adding the app to their profiles.

Conflict caution – The authentication dialog should provide warning signals to the users when data and publishing permissions requested by the app will violate their global privacy settings.

Privacy indication – The authentication dialog should reflect a user's current privacy settings.

The Monochrome Authentication Dialog (MONO) aims to fulfill the first three design principles. Polychrome Authentication Dialog (POLY) is an enhanced version of

Copyright © 2018 IJCSIT.

the MONO design, with a three-color scheme to reflect users' privacy settings, which addresses the fourth design principle (see Figure 6).

The Layout of Permissions: All types of data required by the app are listed in the first column. The first row displays the information regarding how the app will use the data

The Tick Mark and Checkbox: Un-clickable tick marks represent those types of information that will be accessed and used by the app. The checked check box means that users will allow the app to access and use certain information. The un-checked check box means that users will not allow the app to access the corresponding information.

The Red Exclamation Point: When the information requested by the app conflicts with the user's privacy settings, the red exclamation point alerts users about the potential conflict.

GREEN indicates the current privacy setting for the corresponding information is "Everyone" and it will NOT be violated by adding the app to the user's Facebook account.

RED indicates the current privacy setting for that information is "Only Me" or "Specific People…" and it will be violated by adding the app to the user's Facebook account.

YELLOW indicates the current privacy setting for that information is something beyond "Everyone", "Specific People…", or "Only Me" [3].

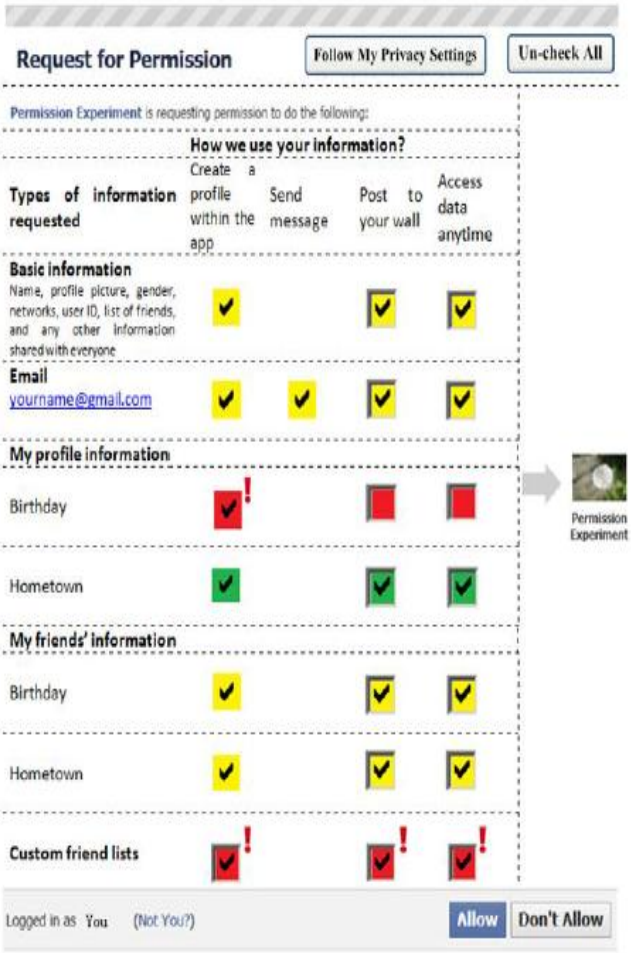


Figure 6. Proposed *POLY* Interface Design.

10. Privacy Model for Third Party Applications on Facebook

"Apps" are the pieces of software that allow Facebook's 500 million users play games or share common interests with one another. The Wall Street Journal found that all of the 10 most popular apps on Facebook were transmitting users' IDs to outside companies.

The apps, ranked by research company include Zynga Game Network Inc.'s FarmVille, Texas HoldEm Poker and FrontierVille. Three of the top 10 apps, including FarmVille, have also been transmitting personal information about a user's friends to outside companies.

Most of the apps aren't made by Facebook, but by independent software developers. The information being transmitted is one of the Facebook's basic building blocks: the unique "Facebook UserId" number assigned to every user on the Facebook. Since a Facebook UserId is a public part of any Facebook profile, anyone can use

Copyright © 2018 IJCSIT.

it to look up a person's name, using a standard Web browser, even if that person has set all of his Facebook information to be private. For other users, the Facebook UserId reveals information they have set to share with "everyone," including age, residence, occupation and photos.

The apps reviewed by the Journal were sending Facebook UserId to at least 25 advertising and data firms, several of which build profiles of Internet users by tracking their online activities. This leads to a privacy breach causing leakage of users' private information. Stealing and abusing privacy information on Facebook enhances the privacy concern of the people.

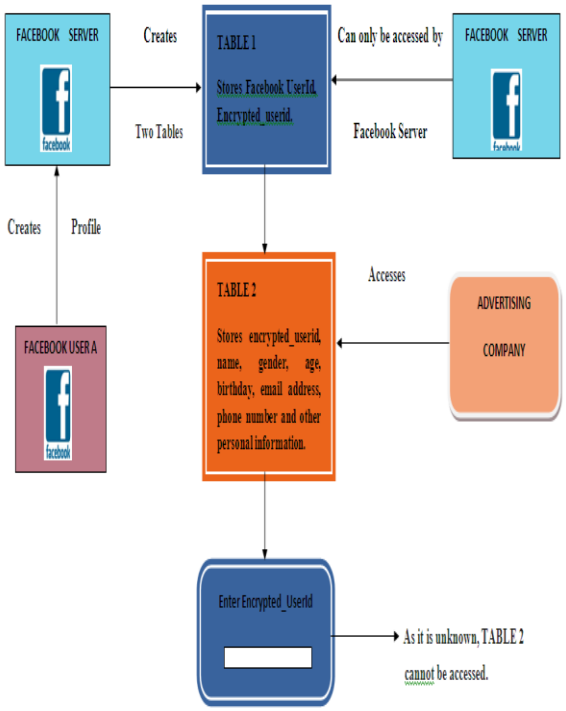


Figure 7. Privacy model for Third Party Applications on Facebook

This privacy risk can be solved by implementing the proposed privacy model. According to the privacy model the Facebook server creates two tables. The Facebook server creates encrypted_ UserId for every UserId created on the Facebook. The first table stores Facebook UserId and encrypted_UserId which should be accessed only by the Facebook server. The second table stores the fields such as encrypted_UserId, name, gender, age, birthday, email address, phone number and other personal information. Only when an advertising company knows the encrypted_UserIds, it can access the personal information of the Facebook users who have opted to use the strictest of privacy settings. The advertising companies cannot access the personal information of the users with their Facebook UserIds. Thus this model protects the privacy of the Facebook users. Figure 7 shows the privacy model for third party applications on Facebook.

11. Comparison of various Privacy Models.

Author Name	Name of the Privacy Model	Features
Sazzadur Rahman	FRAppE	Facebook's Rigorous Application Evaluator—arguably the first tool focused on detecting malicious apps on Facebook
Kiran Bhise	Malignant Facebook Application Predictor	Using FRAppE, it can predict malicious application with better results as compared to an existing system.
Mohamed Shehab	OAuth Model	It uses the concept of Access Tokens to authorize the third party applications
Jonathan Anderson and Frank	Footlights Model	It provides an API that lets applications work with the user data but not leak it beyond the user's consent.
Mohamed Shehab	Access Control Framework	It uses the required user profile attributes to manage third party applications
N. Jayalakshmi	Privacy model for Third Party Applications on Facebook	It protects the profile data of the Facebook users from third party applications.

Foot light Model and OAuth Model authorize the third party application to work with user data but not beyond the user's consent. FRAppE and Malignant Facebook Application Predictor detect malicious applications on Facebook. Access Control Framework uses the required user profile attributes to manage third party applications. Privacy model for Third Party Applications on Facebook protects the profile data of the users from third party applications

11. Conclusion

This paper first presents a survey on different frameworks and improved interface designs which technically enforces the protection of the personal information of a user, when interacting with third party applications on Facebook. It also explains the privacy issues with the

third party applications. The personal information which is leaked by the third party applications can lead to privacy drifts such as damaging the reputation and creditability of the user. The main goal of the paper is to propose a privacy model for third party applications on Facebook that protects the privacy of the users. With the social networking attacks increasing day by day, implementation of this proposed model will surely reduce the number of privacy information stealing and leakage incidents.

REFERENCES:

1. Mohamed Shehab et al., Recommendation Models for Open Authorization, IEEE Transactions on dependable and secure computing, Vol. 9, No. 4, July/August 2012.
2. Jonathan Anderson, Frank, Must Social Networking Conflict with Privacy**,** Co published by the IEEE Computer and Reliability Societies May/June 2013.
3. Na Wang et al., Third-Party Apps on Facebook: Privacy and the Illusion of Control, ACM CHIMIT '11, December 4, 2011, Boston, MA, USA.
4. Mohamed Shehab et al., Access control for online social networks third party Applications, computers & security 3 1 (2 0 1 2) 8 9 7-9 1 1.
5. Sazzadur Rahman et al., Detecting Malicious Facebook Applications, IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 24, NO. 2, APRIL 2016.
6. Jennifer King, Privacy: Is There An App for That?, Symposium On Usable Privacy and Security (SOUPS) 2011, July 20-22, 2011, Pittsburgh, PA, USA.
7. Md Sazzadur Rahman et al., FRAppE: Detecting Malicious Facebook Applications, CoNEXT'12, December 10–13, 2012, Nice, France.
8. Kiran Bhise et al., A Method For Recognize Malignant Facebook Application, ISBN: 978-1-5090-1666-2/16/$31.00 ©2016 IEEE.
9. Na Wang et al., An Online Experiment of Privacy Authorization Dialogues for Social Applications, CSCW '13, February 23–27, 2013, San Antonio, Texas, USA.
10. N. Jayalakshmi, R.G. Kavitha, A Survey on Privacy in Social Networking Websites, IRJET, volume 3, issue 1, January 2016.
11. N. Jayalakshmi, R.G. Kavitha, Privacy in Social Networking Websites, IRJET, volume 2, issue 9, December 2015.