Facebook Application Specificity

Dimple Khatri[1], Shivani Kadam[2], Chandni Kesariya[3], Sudarshan Ghogare [4]
Department of Information Technology
[1, 2, 3, 4] D. Y. Patil College of Engineering, Akurdi

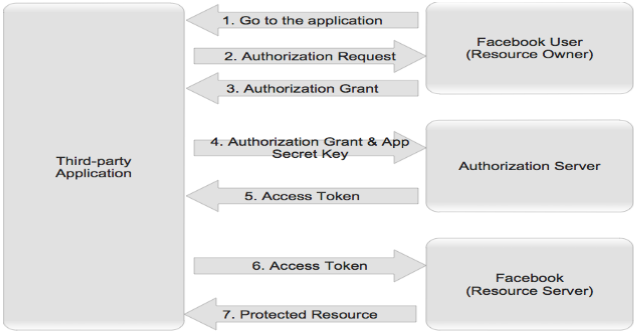
Abstract-*Social networks are driving interest of user's by creating a platform like third party apps. These third-party apps act as an easy platform for hackers to spread malicious contents on social media like Facebook, twitter etc. In this paper, we are going to create an app which can detect malicious apps. Key components of proposed architecture are: (1) Depending upon look alike name trick that can be detected using app id. (2) Depending upon the permission sets, malicious apps often request fewer permission sets. (3) Depending upon URLs – it will determine whether the URL is spam or directs to spam content. Based on these components we detect whether the app is malicious or not. Hackers design app in such a way so that millions of users install the app which provides a mean to spread malicious contents. Hackers create various messages that direct to malicious link when user access those messages. These malicious apps track all the personal information related to social account. Here it will further inform the user about the malicious app so that the user can decide whether to install the app or not.*

Keywords*-*Benign apps, malicious, Social media

I. INTRODUCTION

In recent years, there is a tremendous increase in online social media sites. Online social networks help people to communicate in different ways. OSNs drive the attention of users in day to day life. It is a platform provided to users to share their information, to interact with other users, online businesses. It enables users to create and share content or to participate in social networking. Facebook is an online social networking site that allows users to create their personal profiles, share photos and videos, and communicate with other users. There are more than thousands of apps available on Facebook. The number of apps and websites connected to Facebook is likely to quickly grow past 9 million. Facebook provides API so that developers can integrate apps into Facebook. Some social media sites have greater potential for content that is posted there to spread virallyover social networks. Hackers have started taking advantage of these apps to spread malicious content or for extracting user's personal information. Popularity of these apps depends upon the no of installations. So, hackers have started creating look alike name app so that it drives the attention of the user which helps to spread malicious content or hack the users personal profile. Popularity of apps spread to large no of audience through suggestions and recommendation of friends. So, it spread the malicious contents to large no of users.

In this paper, we are going to create a website which will detect malicious apps depending upon the URL identification, app ID. Client Id during app installation differs. When user clicks on app installation hackers integrate a different link during installing which leads to installation of malicious app. So, we are going to detect malicious app and inform the user before installing the app. Facebook grants permission to applications to access user's personal information by handing overthe OAuth 2.0 protocol to application server for each user who installs the application [7].



The OAuth 2.0 protocol

II. LITERATURE SURVEY

So far, the research community has paid little attention to OSN apps specifically. Most research related to spam and malware on Facebook has focused on detecting malicious posts and social spam campaigns. Gao *et al.* analysed posts on the walls of 3.5 million Facebook users and showed that 10% of links posted on Facebook walls are spam. They also presented techniques to identify compromised accounts and spam campaigns. Yang *et al.* and Benevento *et al.* developed techniques to identify accounts of spammers on Twitter. Others have proposed a honey-pot-based approach to detect spam accounts on OSNs. Yardi *et al.* analysed behavioural patterns among spam accounts in Twitter. Chia *et al.* investigate risk signalling on the privacy intrusiveness of Facebook apps and conclude that current forms of community ratings are not reliable indicators of the privacy risks associated with an app [11].

Operation of Malicious Applications:

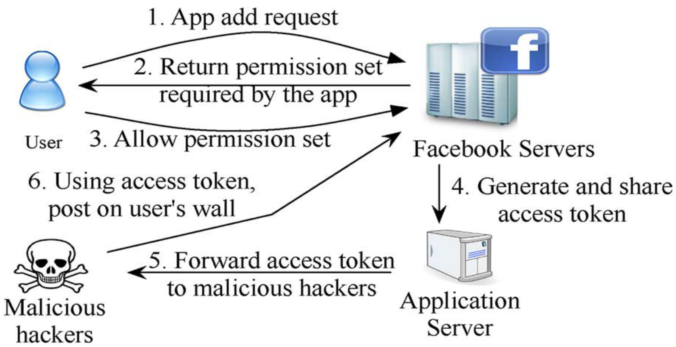

1. App add request
2. Return permission set required by the app
3. Allow permission set
User
Facebook Servers
4. Generate and share access token
6. Using access token, post on user's wall
5. Forward access token to malicious hackers
Malicious hackers
Application Server

Figure 2.1 Steps involved in getting access tokens by malicious apps

Malicious Facebook applications typically operate as follows:
Step 1: Hackers convince users to install the app, usually with some fake promise (e.g., free iPads).

Step 2: Once a user installs the app, it redirects the user to a Web page where the user is requested to perform tasks, such as completing a survey, again with the lure of fake rewards.

Step 3: The app thereafter accesses personal information (e.g., birth date) from the user's profile, which the hackers can potentially use to profit.

Step 4: The app makes malicious posts on behalf of the user to lure the user's friends to install the same app (or some other malicious app, as we will see later). This way the cycle continues with the app or colluding apps reaching more users. Personal information or surveys can be sold to third parties to eventually profit the hackers [11].

Existing system works concentrated only on classifying individual URLs or posts as spam, but not focused on identifying malicious applications that are the main source of spam on Facebook. Existing system works focused on accounts created by spammers instead of malicious application. Existing system provided only a high-level overview about threats to the Facebook graph and do not provide any analysis of the system.

III. RELATED STUDY

Versions of malware that targets Facebook:

1. Facebook Child Video Virus: It is a dangerous application, which is circulating on Facebook in a form of pornographic video. It may seem that the message, which has this video attached, was sent by your friend and it is safe. However, after opening it, it becomes clear that it's related to child pornography. Some victims report that it contains a phrase 'watch this if you're curious'. Once opened, virus automatically attaches to your Facebook account and shares this video with all your Facebook friends.

2. Facebook Colour Change Virus: It is a devious type of the Facebook virus, which relies on a message offering to change your social network's background to pink, red, black or another colour. Just like other types of this threat, it may come to your inbox from one of your contacts, which has also been tricked by this fraud message. Typically, it includes a malicious link helping for scammers to drive more traffic to their online survey. If you click on this link, you will send this fraud message to all your contacts.

3. Facebook Friend Request Virus: It is a dangerous threat, which sends friend requests from user's account to unknown people or, even worse, the ones who have been already blocked by a user. It has been reported that sometimes this virus manages to send more than 100 invites to random people. The point of creating and using this hasn't still been revealed. However, some experts claim that this threat may be used for taking over computers, shutting down their anti-virus programs and similar activities.

4. Facebook Automatic Wall Post Virus: It is a cyber infection, which is created for increasing the traffic to specific domains. Besides, it may negatively affect your computer's security and try to steal your personal information. This virus makes people visit the website by showing a tricky message, which claims 'Sexiest Video ever' and includes a link leading to an unknown website. Besides, it automatically makes a post on your wall and spreads in this way. If you see such message, which seems like it has been posted by your friend, you should remove it from your wall immediately.

5. Facebook Message Virus: It is another variant of Facebook virus, which is spreading via the chat window. This virus pop-ups up with a message, which seems like it's from your friend and includes a normally-looking link. Of course, you should never click on this link because it infects computers with the virus capable of disabling anti-virus software and download further malware on the system. Of course, if you click on a link, this virus will continue spreading itself on your Facebook account.

6. Invitation Facebook Virus: It is a different kind of virus that has been spreading on Facebook for years. It spreads via an emails and Facebook's message board and

announces about a great danger on this social network. To be more precise, it foolishly warns about the Facebook threat that comes as a message with an attachment called Invitation Facebook and 'opens an Olympic torch and will take the whole hard disk C of your computer.' However, our security experts have revealed that this message includes Trojan horse and other types of viruses. You should remove this fraud letter as soon as you receive it.

7. Facebook Stalker Virus: It a dangerous FB application, which is actively spread on this social network. It belongs to scammers and it is used for stealing personal users' information, not for helping people to find out who is secretly watching their FB profile. If you fall for FB Stalker app, you will be rerouted to a malicious site, which looks like a typical login page of the Facebook. Please, do NOT enter your personal information on it because you will lose your personal information and Facebook's account!

8. Facebook “hahaha” Virus: is yet another version of Facebook virus. It is a serious malware, which is spread via this social network and used for turning the computer into a bitcoin mining machine. Once it tricks its victims into downloading a malicious. Zip file, it starts initiating serious system's slowdowns and similar issues. Please, don't let this malicious software stay on your computer because you can never know what malicious activities it can be used for.

9. Facebook video Virus: It is a malicious virus that controls victim's Facebook account and automatically posts "My private video," "My video," "Private video" and similarly entitled malicious links on victim's timeline. What is more, it tags random victim's Facebook friends in these posts to draw their attention and invite them to click on the link. This virus also sends messages including the malicious link directly to victim's friends. We strongly advise you NOT to click on these links as it can automatically download malware to your computer.

IV. SYSTEM ARCITECTURE

Most of the malicious posts on Facebook are spread by third party applications. The malicious apps get many clicks on the URLs they post, that appear on user’s wall or news feed. We compare malicious and benign apps with respect to various features such as:

1) Application Summary: It consists of attributes like category, description, company name. a) Category: We check whether category is provided or not? Category is selected from the predefined list provided by Facebook. b) Company name: We check whether, is it specified? c) Description: It is generally some information provided by the developers regarding what the app is about, its purpose, its usefulness, etc. Most of the benign apps provide this information but malicious apps do not provide such information.

2) Required Permission Set: All the apps request the users to grant some permissions that it requires. It includes permissions like birth date, gender, friend list, etc. Mostly the malicious apps request for less number of permissions. This is the reason many users easily agree to install them.

3) App Name: As every app is configured with a unique App ID so there are no restrictions on App Name and thus many apps have similar names. This misleads the users, as user may unknowingly install malicious apps because its name appears to be very like some popular app on Facebook.

4) Posts on profile page: Any post on Facebook optionally includes URL, most of the malicious apps post link that point to domain or links that are external to or outside Facebook. Benign apps rarely tend to post such kind of links.

5) Client ID and App ID: For them, we check whether both are different from each other or not?

6) Redirect URI: It refers to the URLs where, after installing the app users are redirected to. These malicious apps redirect users to URLs that have poor reputation. Users are redirected towards such URLs on installation of the app.

The basic architecture for differentiating between malicious apps and benign apps is as show in figure

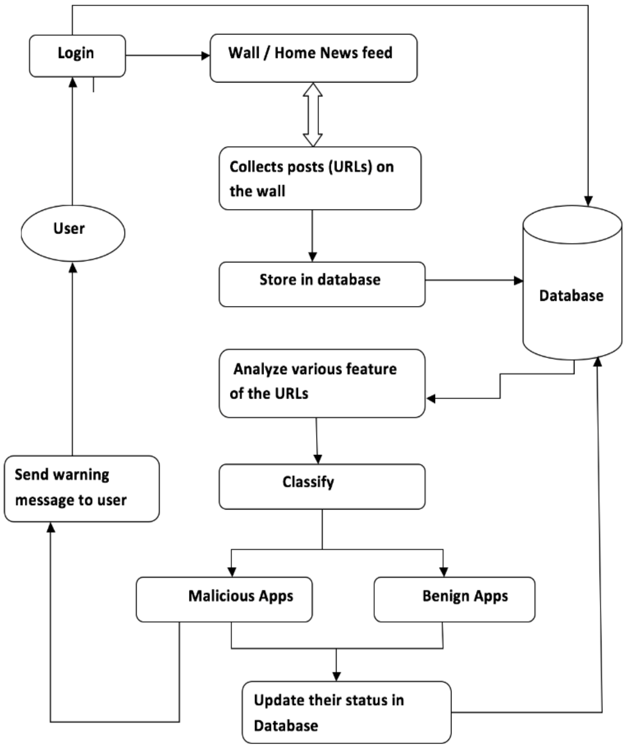

Login
Wall / Home News feed
Collects posts (URLs) on the wall
User
Store in database
Database
Analyze various feature of the URLs
Send warning message to user
Classify
Malicious Apps
Benign Apps
Update their status in Database

Figure 4.1 Architecture to determine specificity of apps on user's wall

Step-1: Here we evaluate every URL posted on user's wall/news feed/home to check whether it is malicious or not based on certain features as mentioned above.
Step-2: Based on analysis of these features we determine whether an app is malicious or benign and accordingly update the information about them in Database.
Step-3: All the obtained URLs that were posted on user's wall/news feed/home are stored in database.
Step-4: Further analysis on this stored information is carried out and the results are then updated and stored for each in the database accordingly. The information stored in database is used for referring whether an app is malicious or not.
Step-5: If the app is found to be malicious then the user is notified about it with the help of a warning message, when its clicks on link to install the app. Next it depends on the user whether he wants to continue with installing that specific app or not.

In this way, the specificity about whether the app on Facebook is malicious or benign is determined.

VI. CONCLUSION

In this paper, we have created a tool/app that detects malicious apps by analysing various features of the URLs. This app will help to classify malicious and benign apps. End users will be aware of the malicious apps before installing it. This will stop promoting and spreading of malicious apps. Here we are only detecting malicious apps and not blocking them. Final decision of installing apps still depends upon the user.

ACKNOWLEDGMENT

We take this opportunity to thank Mr. A. J. Patankar, the Head of the Department (Information Technology) and Mr. K. D. Bamane, the project coordinator, for his valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this project report. We are also thankful to our project guide Mrs. Aarti Gaikwad for her valuable and priceless support. We are thankful to all the staff members of the Department of Information Technology of D. Y. Patil College of Engineering, Akurdi for their valuable time, support, comments, suggestions, and persuasion. We would also like to thank the Institute for providing the required facilities, internet access and important books.

REFERENCES

[1] C. Pring, "100 social media statistics for 2012," 2012 [Online]. Available: http://thesocialskinny.com/100-social-media-statistics-for-2012/

[2] Facebook, Palo Alto, CA, USA, "Facebook Opengraph API," [Online]. Available: http://developers.facebook.com/docs/reference/api/

[3] "Wiki: Facebook platform," 2014 [Online]. Available: http://en.wikipedia.org/wiki/Facebook_Platform

[4] "Pr0file stalker: Rogue Facebook application," 2012 [Online]. Available: https://apps.facebook.com/mypagekeeper/?status=scam_report_fb_survey_scam_pr0file_viewer_2012_4_4

[5] Facebook, Palo Alto, CA, USA, "Facebook platform policies," [Online]. Available: https://developers.facebook.com/policy/

[6] Facebook, Palo Alto, CA, USA, "Application authentication flow using OAuth 2.0," [Online]. Available: http://developers.facebook. com/docs/authentication

[7] N. Wang, H. Xu, and J. Grossklags, "Third-party apps on Facebook: Privacy and the illusion of control," in Proc. CHIMIT, 2011, Art. no.4.

[8] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, “Design and evaluation of a real-time URL spam filtering service,” in Proc. IEEE Symp. Security Privacy, 2011, pp. 447–462.

[9] Facebook, Palo Alto, CA, USA, “Permissions reference,” [Online]. Available: https://developers.facebook.com/docs/authentication/permissions/

[10] Facebook, Palo Alto, CA, USA, “Facebook developers,” [Online]. Available: https://developers.facebook.com/docs/appsonfacebook/tutorial/

[11] Sazzadur Rahman, Ting-Kai Huang, Harsha V. Madhyastha, and Michalis Faloutsos, “Detecting Malicious Facebook Applications”.