International Research Journal of Computer Science (IRJCS)
Issue 05, Volume 4 (May 2017) SPECIAL ISSUE
ISSN: 2393-9842
www.irjcs.com

Security Model for Social Media to Block Unauthorized User

[1]Anil Kumar, Asst. Prof.
[2]Bharath Kumar,[3]Joel, [4]Anees Anthapur,[5]Karthik M,
[1,2,3,4,5]Department of Computer Science and Engineering,
Vemana Institute of Technology, Bengaluru -34

Abstract*—Facebook is one of most used social media, with over 2.2 million users. Hackers have realized potential of using apps to spread malware and spam. Research community has focused on detecting malicious posts and campaigns and not focused on source of malware. FR AppE tool that detects malicious apps on Facebook. To find malicious user and block the malicious user if they are not authorized.

Keywords* — Facebook apps, malicious, online social networks, spam.

I. INTRODUCTION

Facebook one of most widely used social media. Around one million are using facebook. OSN have attracted the facebook user all over the world. Many spam and malicious posts are given by hackers. In this paper we find the malicious user and block the malicious user.

II. RELATED WORK

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.* analyzed 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 Benevenuto *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.* analyzed behavioral patterns among spam accounts in Twitter.Chia *et al.* investigate risk signaling 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. Disadvantage is it 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. Its 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. MODELS

In this paper, we develop FR AppE, a suite of efficient classification techniques for identifying whether an app is malicious or not. To build FR AppE, we use data from MyPage- Keeper, a security app in Facebook. We find that malicious applications significantly differ from benign applications with respect to two classes of features: On-Demand Features and Aggregation-Based Features.We present two variants of our malicious app classifier— FR AppE Lite and FR AppE.FR AppE Lite is a lightweight version that makes use of only the application features available on demand. Given a specific app ID, FR AppE Lite crawls the on-demand features for that application and evaluates the application based on these features in real time FR AppE—a malicious app detector that utilizes our aggregation-based features in addition to the on-demand features.

A. System Model

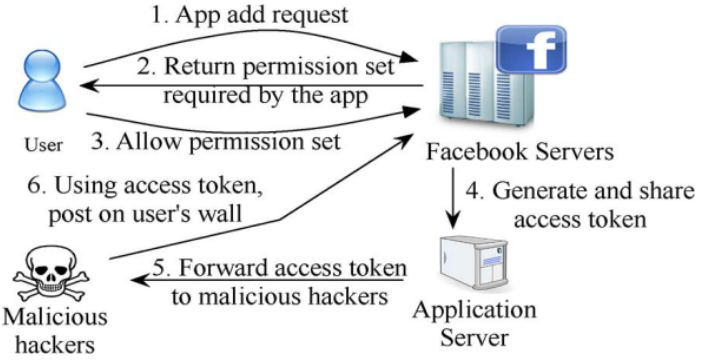


Fig. 1. Steps involved in hackers using malicious applications to get access tokens to post malicious content on victims' walls.

Fig. 1 depicts the steps involved in the installation and operation of a Facebook application. Operation of Malicious Applications: 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.*
- *Step4: 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 and more users. Personal information or surveys can be sold to third parties to eventually profit the hackers.*

B. System Requirement

It specifies the hardware and software requirements that are required in order to run the application properly. The Software Requirement Specification (SRS) is explained in detail, which includes overview of this dissertation as well as the functional and non-functional requirement of this dissertation

Functional	Admin login by using valid user name & password, he can do some operations such as add domain, add projects, assign projects, view all bugs, list all projects, list all assigned projects, list all users, view searched history. After registration successful he has to login by using authorized user name and password. Login successful he will do some operations like view my details, view project assigned, view send bug report, view all bugs, list search other bugs, list my searched history and log out.
Non- Functional	Admin never monitors the user activities
External interface	LAN , WAN
Performance	Admin login, User login, List of All Search History, list all projects, list all assigned projects, list all users.
Attributes	Bug ID, domain, defects, bug reports, instance selection, feature selection, bug data reduction.

Table1: Summaries of SRS

Functional Requirements

Functional Requirement defines a function of a software system and how the system must behave when presented with specific inputs or conditions. These may include calculations, data manipulation and processing and other specific functionality. In this system following are the functional requirements:-

The Admin has to login by using valid user name and password.
After admin login successful he can do some operations such as add domain, add projects, assign projects, view all bugs, list all projects, list all assigned projects, list all users, view searched history.
Admin can add the domain. If the admin want add the domain, he will enter domain name and click on submit button. The details will be stored in the database.

When the admin wants to add projects, he clicks on add projects and enter project name, project description, domain name, start date, end date and project image and click on submit button the details will be stored in the data base.
User should register before doing some operations. After registration successful he has to login by using authorized user name and password. Login successful he will do some operations like view my details, view project assigned, view send bug report, view all bugs, list search other bugs, list my searched history and logout.
When user clicks on send bug report button, he will select the project and clicks on submit button, then he will enter developer name, project name, project description, domain, start date, end date, select bug type, enter bug description and click on assign button, the corresponding details will be stored.

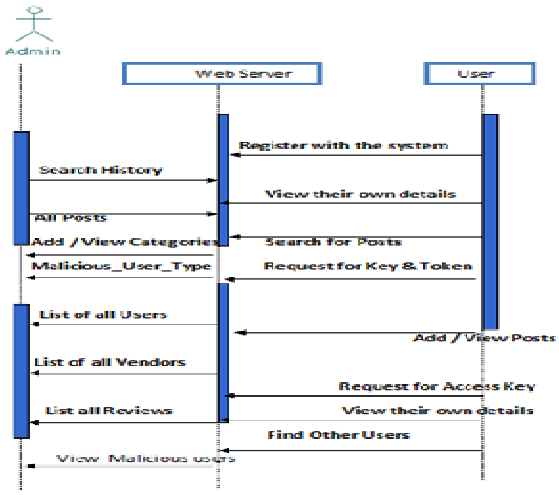
Non – Functional Requirements

Non – Functional requirements, as the name suggests, are those requirements that are not directly concerned with the specific functions delivered by the system. They may relate to emergent system properties such as reliability response time and store occupancy. Alternatively, they may define constraints on the system such as the capability of the Input Output devices and the data representations used in system interfaces.

Many non-functional requirements relate to the system as whole rather than to individual system features. This means they are often critical than the individual functional requirements. The following non-functional requirements are worthy of attention.

THE KEY NON-FUNCTIONAL REQUIREMENTS ARE:
Security: The system should allow a secured communication between server, Admin and users.
Energy Efficiency: The Energy consumed by the Users to receive the File information from the server and admin.
Reliability: The system should be reliable and must not degrade the performance of the existing system and should not lead to the hanging of the system.

IV. BACKGROUND



Home page includes Admin login,User Login,Register New User.
Home page includes all the research and survery results, Actual data and analysis of the facebook malware and spams.
The application should be deployed on the server. Here we are using apache tomcat V6.0 and deployed on the local machine.
New user of the application and the existing users can login to the application.
The user has to enter all the details and submit the form.
The form will be validated by the admin.

A. ADMIN LOGIN

Admin reserves all the right to authenticate or unauthenticated the users.
Admin of the application has to enter with valid credentials.
Admin reserves all rights to authenticate the user. The valid users will be authenticated and given access, in the same time authentication of all misbehaving users should be blocked.
Once admin login to the application, Admin will be provided with a set of rights using which he will authenticate the users.
Admin can see list of users using the application and their post ranking.
While validating the user, If user is valid he can approve and authenticate. The authenticate users can have a token key, which should be used during any kind of operation like posting the product. Admin can view all the friend request. The malicious users will be listed by Admin based on different authentication levels.
Without generating the secret key if the user is accessing the application, then he is will be blocked and informed to the user.
Without any kind of Authentication, If the user tries to access the system by searching the posts which other users already posted, then such users will be blocked and un authorised. In both the cases, if the user is malicious then it will be informed appropriately.

B. USER LOGIN

User has to login with the Right credentials, If the admin did not authorize, then even for trusted users the data will be encrypted. Once the authentication is done, the proper data will be displayed to the end user. Each user has set of permissions which is as shown in the next slide**.** If the user is authenticated then User authentication status will be displayed and along with secret key if it is generated by admin. Valid user can add post, before adding the user should enter the valid key or token. Unauthenticated users cannot add the post. Valid user can view all posts, which he has posted previously and search for the post. User can see the friend request and can accept or reject the request made.User can logout from the application.

V. CONCLUSION

In this paper, we detect the malicious user and block the malicious user we detect the malicious user if they are not authorized by the admin. If the admin authorize the user with the application ID or token or secret key then the user will be Benign and can post the message, comment ,view all the post ,search for the post ,can accept or reject the request made by other.

VI. 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]. "Profile stalker: Rogue Facebook application," 2012 [Online]. Available: https://apps.facebook.com/mypagekeeper/?status=scam_report-_fb_survey_scam_pr0file_viewer_2012_4_4
[5]. "Whiich cartoon character are you—Facebook survey scam," 2012 [Online]. Available:https://apps.facebook.com/mypagekeeper/?status=scam_report_fb_survey_scam_whiich_cartoon_character_are_you_2012_03_30
[6]. G.Cluley,"The Pink Facebook rogue application and survey scam," 2012 [Online]. Available: http://nakedsecurity.sophos.com/2012/02/ 27/pink-facebook-survey-scam/
[7]. D.Goldman, "Facebook tops 900 million users," 2012 [Online]. Available: http://money.cnn.com/2012/04/23/technology/facebookq1/ index.htm
[8]. R. Naraine, "Hackers selling $25 toolkit to create malicious Facebook apps," 2011 [Online]. Available: http://zd.net/g28HxI
[9]. HackTrix, "Stay away from malicious Facebook apps," 2013 [Online]. Available: http://bit.ly/b6gWn5
[10]. M. S. Rahman, T.-K. Huang, H. V. Madhyastha, and M. Faloutsos, "Efficient and scalable socware detection in online social networks," in *Proc. USENIX Security*, 2012, p. 32.

