RESEARCH ARTICLE OPEN ACCESS

Discovery of Ranking Frauds for Mobile Apps Using FRAppE Tool

Dr. L. Pavithira MCA, M.Phil., Ph.D.
Associate Professor
Department of Computer Applications
CMS College of Science and Commerce
Chinnavedampatti, Coimbatore
Tamil Nadu – India

ABSTRACT

We are all living in a technology era. Were it is necessity of using smart phones with all kind of online mobile applications like Facebook, whatsapp, twitter etc. In this now Facebook application installs 20 million a day and it's an important online social network which is an easy way people used to communicate each other. The major reason for tremendous popularity and addictiveness for Facebook app is third party applications. Unfortunately, hackers have realized the potential of using apps for spreading malware and spam. The problem is already significant, as we find that at least 13% of apps in our dataset are malicious. In this paper we propose to identify malicious apps using FRAppE (Facebook's Rigorous Application Evaluator) tool. We explore the ecosystem of malicious Face book apps and identify mechanisms that these apps use to propagate. Long term, we see FRAppE as a step toward creating an independent watchdog for app assessment and ranking, so as to warn Face book users before installing apps.

Keywords:- ONLINE Social Networks (OSNs), Facebook, Malicious Apps, Spam, Hackers.

1. INTRODUCTION

1.1 Online Social Networks (OSNs)

ONLINE social networks (OSNs) enable and encourage third-party applications (apps) to enhance the user experience on these platforms. Such enhancements include interesting or entertaining ways of communicating among online friends and diverse activities such as playing games or listening to songs. For example, Facebook provides developers an API that facilitates app integration into the Facebook user-experience. There are 500K apps available on Facebook, and on average, 20M apps are installed every day. Furthermore, many apps have acquired and maintain a really large user base. For instance, Farmville and City Ville apps have 26.5M and 42.8M users to date. Recently, hackers have started taking advantage of the popularity of this third-party apps platform and deploying malicious applications. Malicious apps can provide a lucrative business for hackers, given the popularity of OSNs, with Facebook leading the way with 900M active users. There are many ways that hackers can benefit from malicious apps using online social networks.

1.2 Malicious Applications in OSNs

In other words, the problem is the following: Given an app's identity number (the unique identifier assigned to the app by Facebook), can we detect if the app is malicious? Currently, there is no commercial service, publicly available information, or research-based tool to advise a user about the risks of an app., malicious apps are widespread and they easily spread, as an infected user jeopardizes the safety of all its friends. So far, the research community has paid little attention to OSN apps specifically. Most of the research related to spam and malware on Facebook has focused on detecting malicious posts and social spam campaigns. At the same time, in a seemingly backwards step, Facebook has dismantled its app rating functionality recently. A recent work studies how app permissions and community ratings correlate to privacy risks of Facebook apps. Finally, there are some community-based feedback-driven efforts to rank applications, such as WhatApp?; though these could be very powerful in the future, so far they have received little adoption.

1.3 Malicious Apps in Facebook Applications

There are many ways that hackers can spread and get benefit from malicious apps using Facebook application for example,

- The app can reach large numbers of users and their friends to spread spam.
- The app can obtain users' personal information such as e-mail address, home town, and gender.
- The app can "reproduce" by making other malicious apps popular.

To make matters worse, the deployment of malicious apps is simplified by ready-to-use toolkits starting at $25. In other words, there is

motive and opportunity, and as a result, there are many malicious apps spreading on Facebook every day. Despite the above worrisome trends, today a user has very limited information at the time of installing an app on Facebook. Hackers can easily get large number of data or and personal information from many users using to spread these malicious apps.

II. DETECTING MALICIOUS APP

In an Existing system ONLINE social networks (OSNs) enable and encourage third-party applications (apps) to enhance the user experience on these platforms. Recently, hackers have started taking advantage of the popularity of this third-party apps platform and deploying malicious applications. Malicious apps can provide a lucrative business for hackers, given the popularity of OSNs, with Face book leading the way with 900M active users. There are many ways that hackers can benefit from a malicious app: 1) the app can reach large numbers of users and their friends to spread spam; 2) the app can obtain users' personal information such as e-mail address, home town, and gender; and 3) the app can "reproduce" by making other malicious apps popular. To make matters worse, the deployment of malicious apps is simplified by ready-to-use toolkits starting at $25. In other words, there is motive and opportunity, and as a result, there are many malicious apps spreading on Facebook every day. The main disadvantages in existing systems are,

- Hackers Spreading malware and spam in Facebook using app.
- Many malicious apps spreading on Facebook

To identify malicious Facebook Applications we present two variants of our malicious app classifier FRAPPE lite and FRAPPE. FRAPPE Lite is a lightweight version that makes use of only the application features available on demand. Given a specific app ID, FRAPPE Lite crawls the on-demand features for that application and evaluates the application based on these features in real-time. FRAPPE is a malicious app detector that utilizes our aggregation-based features in addition to the on-demand features.

Fig.1Malicious app in Facebook settings

2.1 FRAppE Tool (Facebook's Rigorous Application Evaluator)

Given a Face book application, we determine if it is malicious? Our key contribution is in developing **FRAppE—Facebook's Rigorous Application Evaluator**—the tool focused on detecting malicious apps on Face book. Here we use the "**serial variant evasion technique"** for detecting the malicious code. We explore the ecosystem of malicious Face book apps and identify mechanisms that these apps use to propagate. Long term, we see FRAppE as a step toward creating an independent watchdog for app assessment and ranking, so as to warn Face book users before installing apps.

Were we develop FRAppE, a suite of efficient classification techniques for identifying whether an app is malicious or not. To security app in Facebook that monitors the Facebook profiles of 2.2 million users. We analyze 111K apps that made 91 million posts over 9 months. This is the comprehensive study focusing on malicious Facebook apps that focuses on quantifying, profiling, and understanding malicious apps and synthesizes this information into an effective detection approach.

2.2 Malicious Apps Ecosystem

In this section, we conduct a forensics investigation on the malicious app ecosystem to identify and quantify the techniques used in this cross promotion of malicious apps.

Background on App Cross Promotion: Cross promotion among apps, which is forbidden as per Face book's platform policy, happens in two different ways. The Promoting app can post a link that points directly to another app, or it can post a link those points to a redirection URL, which points dynamically to any one of a set of apps. Promotion Graph Characteristics: From the app promotion dataset we collected above,

We construct a graph that has an undirected edge between any two apps that promote each other via direct or indirect promotion. We refer to this graph as the "Promotion graph".

2.3 Apps Collaboration

We attempt to identify the major hacker groups involved in malicious app collusion. For this, we consider different variants of the "Campaign graph" as follows.

- Posted URL Campaign: Two apps are part of a campaign if they post a common URL.
- Hosted Domain Campaign: Two apps are part of a campaign if they redirect to the same domain once they are installed by a user. We exclude apps that redirect to apps.facebook.com.

We develop FRAppE, a suite of efficient classification techniques for identifying whether an app is malicious or not. To build FRAppE, we use data from My Page- Keeper, a security app in Facebook that monitors the Facebook profiles of 2.2 million users. We analyze 111K apps that made 91 million posts over 9 months. This is arguably the first comprehensive study focusing on malicious Facebook apps that focuses on quantifying, profiling, and understanding malicious apps and synthesizes this information into an effective detection approach. Facebook's Rigorous Application Evaluator—arguably the first tool focused on detecting malicious apps on Facebook.

2.4 Hosting Domain

We investigate the hosting domains that enables redirection web sites. First, we find that most of the links in the posts are shortened URLs, and 80% of them use the bit.ly shortening service. We consider all the bit.ly URLs among our dataset of indirection links (84 out of 103) and resolve them to the full URL. We find that one-third of these URLs are hosted on amazonaws.com. Second, we find that 20% of the domains hosting malicious apps each host at least 50 different apps. This shows that hackers heavily reuse domains for hosting malicious apps.

2.5 Cross Promotion as a Sign of Malicious Intentions

Thus far, we studied cross promotion among malicious apps based on posts marked as malicious by **MyPageKeeper.** However, MyPageKeeper may have failed to flag the posts of many malicious apps. Therefore, here we study the prevalence of cross promotion simply by observing whether the post made by an app includes a URL that points to another app. This enables us to discover a new set of malicious apps that we have failed to identify so far.

III. RELATED WORKS

3.1 input Design for FRAppE tool

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

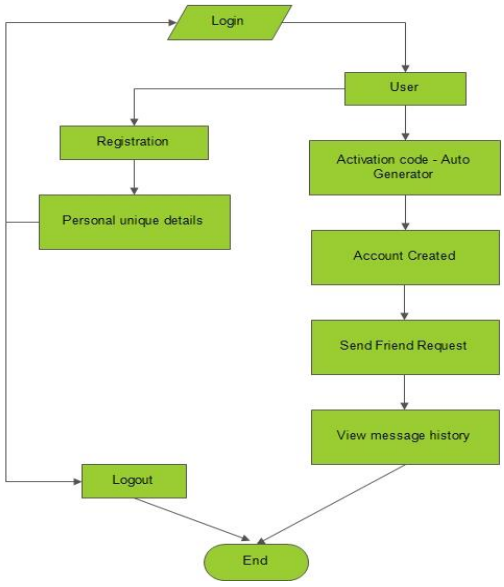

Fig.2 The Framework of the Process to create Facebook Account with unique ID.

Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system. It is achieved by creating user-friendly screens for the data entry to handle large volume of data.

The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

3.2 Output process

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

- Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
- Select methods for presenting information.
- Create document, report, or other formats that contain information produced by the system.
- Convey information about past activities, current status or projections of the

3.3 Table Design

Database is a major part of all the systems. All the data required to produce the various reports like ranking fraud report, fraud count report etc. are stored in database only. From the database, the reports are produced according to the user's requirement. Database design is the process of producing a detailed data model of a database.

TABLE1. MESSAGE PRIMARY KEY: ID

Field	DataType
Id	int (11)
Sender	varchar (50)
Reciver	varchar (50)
Msg	varchar (100)

TABLE2. FRIENDREQUEST PRIMARY KEY: ID

Field	DataType
Id	int (11)
User	varchar (50)
Friend	varchar (50)
location	varchar (50)
status	varchar (50)

TABLE3. USERNAME (VIRTUAL) PRIMARY KEY: ID

Field	DataType	
user_id	int (10)	
Friends	varchar (40)	
Loc	varchar (30)	
friend_request	int (10)	
Message	Text	
secret_code	int (7)	
Sender	varchar (20)	

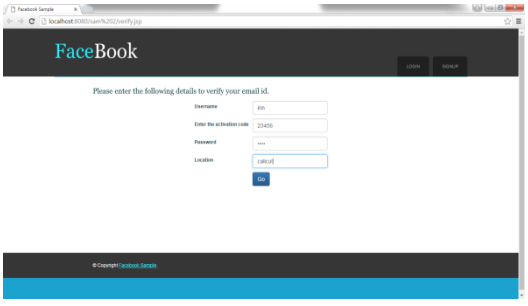

Fig.3 Collect user information

Databases are designed to offer an organized mechanism for storing, managing and retrieving information. They do so through the use of tables. Each table consists of a number of rows, each of which corresponds to a single database record. The database management system will enforce the uniqueness of the key by using the primary key.

IV. SYSTEM IMPLEMENTATION

System implementation is the stage of the project where the theoretical design is turned in to a working system. If the implementation stage is not properly planned and controlled it can chaos. Us it can be considered to be most crucial stage in achieving a new successful system and giving the user's confident that the new system will work and be effective and accurate. It is less creative than system design.

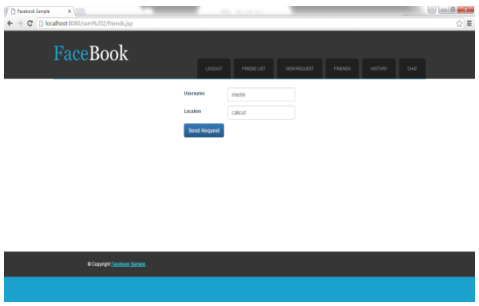

Fig.4 Send Friend Request

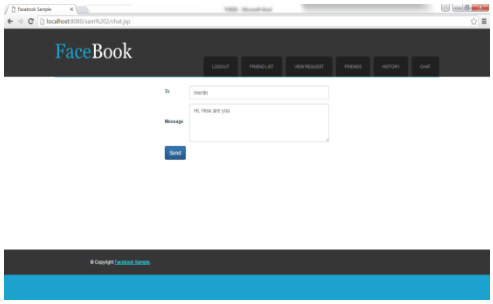

Fig.5 Sending Messages

Implementation primarily concerned with user training and documentation. Depending on the nature of the system extensive users training may be required. Conversion usually takes place about the same time the user is being trained or later. Implementation simply means converting a new system design into operation. An important aspect of system analyst's job is to make sure that the new design is implemented to establish standards. Implementation means the process of converting a new revised system design into an operational one.

At the beginning of the development phase, a preliminary implementation plan is created to schedule and manage the many different activities that must be integrated into plan. The implementation plan updated throughout the development phase, culminating in a change over for the operation phase. The major elements of the implementation plan are test plan, training plan, equipment installation plan and a conversion plan.

- Implementation of a new computer system to replace an existing one.
- Implementation of modified application to replace an existing one.
- Implementation of a computer system to replace a manual.

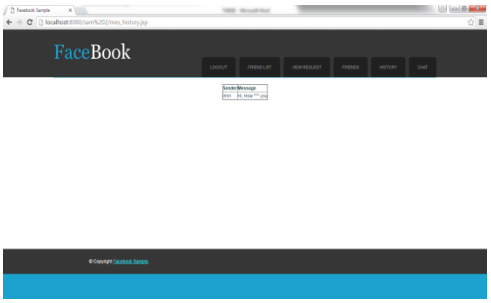

Fig.6 Experimental output

A software application in general is implemented after navigating the complete life cycle method of a project. Various life cycle processes such as requirement analysis, design phase, verification, testing and finally followed by the implementation phase results in a successful project management. The software application has been successfully implemented after passing various life cycle processes mentioned above.

V. CONCLUSION

Applications present convenient means for hackers to spread malicious content on Facebook. However, little is understood about the characteristics of malicious apps and how they operate. In this paper, using a large corpus of malicious Facebook apps observed over a 9-month period, we showed that malicious apps differ significantly from benign apps with respect to several features. For example, malicious apps are much more likely to share names with other apps, and they typically request less permission than benign apps. Leveraging our observations, we developed FRAppE, an accurate classifier for detecting malicious Facebook applications. Most interestingly, we highlighted the emergence of app-nets—large groups of tightly connected applications that promote each other.

REFERENCES

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

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

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

[4] [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] [5] "Which 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] [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] [7] D. Goldman, "Facebook tops 900 million users," 2012 [Online]. Available: http://money.cnn.com/2012/04/23/technology/facebookq1/ index.htm

[8] [8] R. Naraine, "Hackers selling $25 toolkit to create malicious Facebook apps," 2011 [Online]. Available: http://zd.net/g28HxI

[9] [9] HackTrix, "Stay away from malicious Facebook apps," 2013 [Online]. Available: http://bit.ly/b6gWn5

[10] [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.

[11] [11] H. Gao *et al.*, "Detecting and characterizing social spam campaigns," in *Proc. IMC*, 2010, pp. 35–47.

[12] [12] H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary, "Towards online spam filtering in social networks," in *Proc. NDSS*, 2012.

[13] [13] P. Chia, Y. Yamamoto, and N. Asokan, "Is this app safe? A large scale study on application permissions and risk signals," in *Proc. WWW*, 2012, pp. 311–320.

[14] [14] "WhatApp? (beta)—A Stanford Center for Internet and Society Website with support from the Rose Foundation," [Online]. Available: https://whatapp.org/facebook/

[15] [15] "MyPageKeeper," [Online]. Available: https://www.facebook.com/apps/application.php?id=167087893342260

[16] [16] Facebook, Palo Alto, CA, USA, "Facebook platform policies," [Online]. Available: https://developers.facebook.com/policy/

[17] [17] Facebook, Palo Alto, CA, USA, "Application authentication flow using OAuth 2.0," [Online]. Available: http://developers.facebook.com/docs/authentication/

[18] [18] "11 million bulk email addresses for sale—Sale price $90," [Online]. Available: http://www.allhomebased.com/BulkEmailAddresses.htm

[19] [19] E. Protalinski, "Facebook kills app directory, wants users to search for apps," 2011 [Online]. Available: http://zd.net/MkBY9k

[20] [20] SocialBakers, "SocialBakers: The recipe for socialmarketing success," [Online]. Available: http://www.socialbakers.com/

[21] [21] "Selenium—Web browser automation," [Online]. Available: http://seleniumhq.org/