ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Security Protection for Facebook Users from Social Malware

Dr.Chandramouli H, Dr. Josephine Premkumar, Kesavan MV, B Vishwanatha,

Prof. and HOD (R&D), Department of CSE, East Point College of Engineering& Technology, Bangalore, India

Prof. and Head, Department of CSE, East Point College of Engineering & Technology, Bangalore, India

Assistant Professor, Department of CSE, East Point College of Engineering & Technology, Bangalore, India

Assistant Professor, Department of CSE, East Point College of Engineering & Technology, Bangalore, India

Project funded by the Government of Karnataka under VGST Scheme (2014-2018)*

ABSTRACT: Nowadays among Online Social Networks (OSN), Facebook is the widespread one and it is used by 1.5 billion people across the world. Hackers are finding many new ways to propagate spam and malware on these platforms, which we refer to as social malware. They can easily access the personal details. Social malware cannot be identified with existing security mechanisms (e.g. URL blacklists). The developed tool is to protect Facebook users from social malware. The tool can detect malicious apps with complete accuracy. The objective of this project is to detect malicious application and block those applications in Facebook using the implemented tool under the set of constraints. It provides only a high-level explanation about threats to the Facebook graph. The main disadvantage of existing system is the missing security aspect. In the proposed system certain techniques are implemented by which Offensive words or any posts are detected and blocked with the help of dictionary using filters. These words will not be displayed in public wall; instead such post will be automatically migrated to blocked post list. Also a warning mail is will be sent to the user. The user can view it secretly. It is safe and secure.

KEYWORDS: OSN (Online Social Network),JFC (Java Foundation Classes), JDT (Java Development Tools), EFS(Encrypting File System),IPSec (IP Security) GUI (Graphical User Interface), MVC (Model view Controller), DFD (Data Flow Diagram), JVM (Java Virtual Machine). FB (Facebook).

I. INTRODUCTION

Online social networks (OSN) enable and encourage third party applications (apps) to enhance the user experience on these platforms. Such enhancements will 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 [10] that facilitates app integration into the Facebook user-experience. There are 500K apps available on Facebook [11], and on average, 20M apps are installed everyday [1]. Furthermore, many apps have acquired and maintain a large user base. For instance, FarmVille and CityVille apps have 26.5M and 42.8M user's to date. Recently, hackers have started taking advantage of the popularity of this third-party apps platform and deploying malicious applications [15]. Malicious apps can provide a lucrative business for hackers, given the popularity of OSNs, with Facebook is leading way with 900M active users [12]. There are many ways that hackers can benefit from a malicious app. (a) the app can reach large numbers of users and their friends to spread spam. (b) The app can obtain users personal information such as email address, home town, and gender. (c) The app can "re-produce" 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 [12]. In other words, there is motive and opportunity and as a result, there are many malicious apps spreading on Facebook every day [7].

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

II. SURVEY WORK

Detecting and Characterizing Social Spam Campaigns.
Authors: HongyuGao, Jun Hu, Christo Wilson, Zhichun Li, Yan Chen, Ben Y. Zhao.
Description: Authors presented a primary study to calculate and analyze spam campaigns launched on online social networks. They calculated a huge anonym zed dataset of asynchronous "wall" messages in between Facebook users. System detected generally 200,000 malicious wall posts with embedded URLs, originating from more than 57,000 user accounts. Authors found that more than 70% of all malicious wall posts advertise phishing sites. To study the distinctiveness of malicious accounts, and see that more than 97% are compromised accounts, rather than "fake" accounts formed solely for the principle of spamming. Finally, when adjusted to the local time of the sender, spamming dominates actual wall post in the early morning hours when users are feel good in public from the social spam activities.

Is this App Safe? A Large Scale Study on Application Permissions and Risk Signals.
Authors: Pern Hui Chia, Yusuke Yamamoto, N.Asokan.
Description: Third-party applications capture the attractiveness of web and platforms providing mobile application. Many of these platforms accept a decentralized control strategy, relying on explicit user consent for yielding permissions that the apps demand. Users have to rely principally on community ratings as the signals to classify the unsafe and inappropriate apps even though community ratings classically reflect opinions regarding supposed functionality or performance rather than concerning risks. To study the advantages of user-consent permission systems through a large data collection of Facebook apps, Chrome extensions and Android apps. The study confirms that the current forms of community ratings used in app markets today are not reliable for indicating privacy risks an app creates. It is found with some evidences, indicating attempts to mislead or entice users for granting permissions free applications and applications with mature content request "look alike" applications which have similar names as that of popular applications also request more permissions than is typical. Authors find that across all three platforms popular applications request more permission will have more than the average.

Social Applications: Exploring A More Secure Framework.
Authors: Andrew Besmer, Heather Richter Lipford,MohamedShehab, Gorrell Cheek
Description: OSNs such as Orkut, Facebook and others have grown-up rapidly, with hundreds to millions of active users. A new feature provided on several sites is social applications and services written by third party developers that supply additional functionality linked to a user's profile. However, present application platforms put users at risk by permitting the discovery of huge amounts of personal data and information to these applications and their developers. This paper generally abstracts main view and defines the current access control model gave to these applications, and builds on it to generate a more secure framework.

III. EXISTING SYSTEM

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 a malicious app.
Liabilities:-
(a) The app can reach large numbers of users and their friends to spread spam,
(b) The app can obtain users' personal information such as email address, home town, and gender, and
(c) The app can "re-produce" by making other malicious apps popular.

IV. PROPOSED SYSTEM

In this work, a suite of effective grouping systems for distinguishing whether an application is noxious or not. We utilize information from MyPageKeeper, a security application in Facebook that screens the Facebook profiles of 2.2 million clients. We dissect 111K applications that made 91 million posts more than nine months. This is ostensibly the

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

principal far reaching study concentrating on vindictive Facebook applications that spotlights on evaluating, profiling, and understanding pernicious applications, and orchestrates this data into a viable location approach.

Fig 1: Demonstration of System Engineering

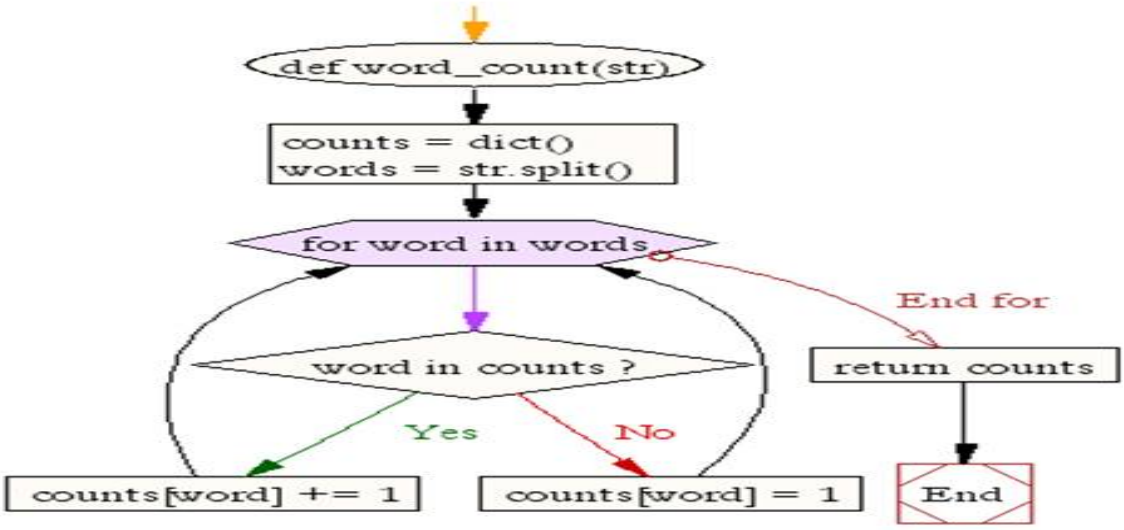

Fig 2: Search Algorithm

The proposed framework in the figure shows the sequence of processes that need to be followed for continues detection of fake profiles with active leaning from the feedback of the result given by the classification algorithm. This framework can easily be implemented by the social networking companies.

1. The detection process starts with the selection of the profile that needs to be tested.
2. After selection of the profile, the suitable attributes (i.e. features) are selected on which the classification algorithm is implemented.
3. The attributes extracted is passed to the trained classifier. The classifier gets strained regularly as new training data is feed into the classifier.
4. The classifier determines the whether the profile is fake or real.
5. The classifier is accurate in classifying the profile so the feedback of the result is given back to the classifier. For example, if the profile is identified as fake, social networking site can send notification to the profile to submit identification. If the valid identification is given, feedback is sent to the classifier that the profile was not fake.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

6. This process repeats and as the time proceeds, the no. of training data increases and the classifier becomes more and more accurate in predicting the fake profiles.

This how we search and compare words in the large amount of data **S**earch in a sorted array to find an item in a sorted array. To do so, look at the array element in the middle. If it contains the item you are seeking, you are done otherwise, and you eliminate either the sub array before or after the middle element from consideration and repeat.

V. PROCESS DESIGN MODEL

The design method that has been followed to design the architecture of the system is MVC design pattern. Swing uses the model-view-controller (MVC) architecture as the fundamental design behind each of its components. Essentially, MVC breaks GUI component into three elements. Each of these elements plays a crucial role in how the component behaves. The MVC design pattern separates a software component into three distinct pieces: a model, a view, and a controller. The model is the piece that represents the state and low-level behavior of the component. It manages the state and conducts all transformations on that state. The model has no specific knowledge of either its controllers or its views. For example, the model of a scrollbar component might contain information about its current position of its adjustable "thumb", its minimum and maximum values, and the thumb's width. A menu on the other hand, may simply contain a list of the menu items the user can select from. The system itself maintains links between model and views and notifies the views when the model changes state. However the title bar may have a close box on the left side or on the right side. These are the examples of different types of views for the same window object.

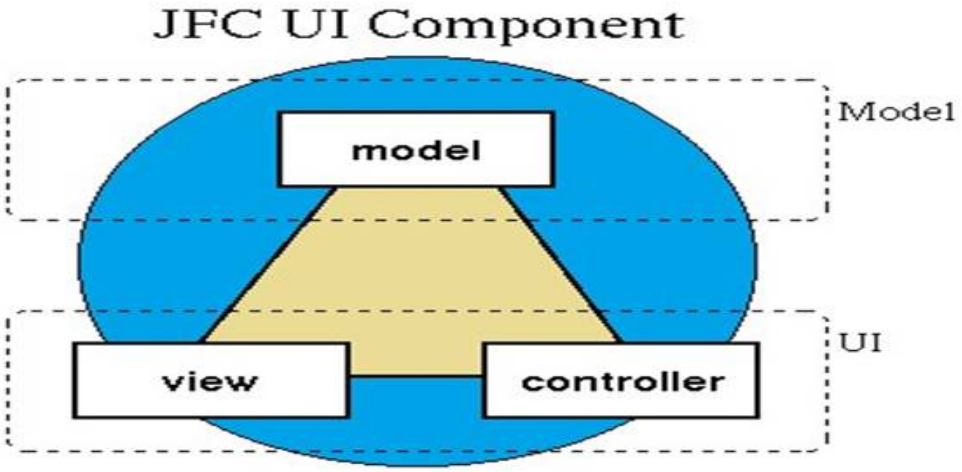

Fig. 3: JFC User Interface Component

Necessity Analysis: This stage is worried about accumulation of prerequisite of the framework. This procedure includes creating record and necessity survey.
Framework Design: Keeping the necessities as a main priority the framework details are made an interpretation of into a product portrayal. In this stage the originator stresses on:- calculation, information structure, programming design and so on.
Coding: In this stage software engineer begins his coding with a specific end goal to give a full portray of item. At the end of the day framework details are just changed over into machine coherent process code.
Execution: The usage stage includes the genuine coding or programming of the product. The yield of this stage is ordinarily the library, executables, client manuals and extra programming documentation.
Testing: In this stage all projects (models) are coordinated and tried to guarantee that the entire framework meets the product prerequisites. The testing is worried with confirmation and approval.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Support: The upkeep stage is the longest stage in which the product is refreshed to satisfy the changing client require, adjust to suit change in the outside condition, redress blunders and oversights beforehand undetected in the testing stage, upgrade the productivity of the product.

A data-flow diagram (DFD) is a graphical representation of the "flow" of data through an information system. DFDs can also be used for the visualization of data processing (structured design). On a DFD, data items flow from an external data source or an internal data store to an internal data store or an external data sink, via an internal process.

A context-level or level 0 data flow diagram shows the interaction between the system and external agents which act as data sources and data sinks. On the context diagram (also known as the Level 0 DFD) the system's interactions with the outside world are modeled purely in terms of data flows across the system boundary. The context diagram shows the entire system as a single process, and gives no clues as to its internal organization.

The Level 1 DFD shows how the system is divided into sub-systems (processes), each of which deals with one or more of the data flows to or from an external agent, and which together provide all of the functionality of the system as a whole. It also identifies internal data stores that must be present in order for the system to do its job, and shows the flow of data between the various parts of the system.

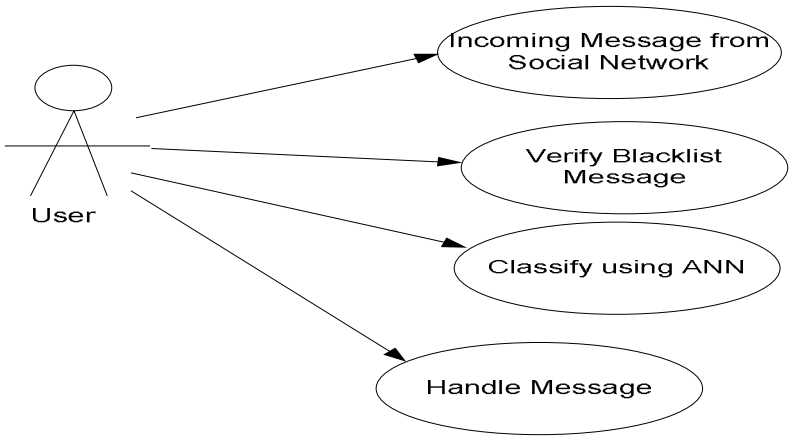

Fig 4: Use Case Diagram for Network Access.

User will send the incoming message from to the system that it will be good for the data accountants for good data will be more it has been good for the anti-social activities on the system more evenly data will verified by the program to classify ANN. Then finally handling the data will be more in this networking system for the users to good social activities will be more it has been very highly effectively it has been good at his more calcified on the accounts and will be done.

VI. CONCLUSION

Applications present a 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 work, using a large corpus of malicious Facebook apps observed, over a nine 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 Facebook App, an accurate classifier for detecting malicious Facebook applications. Most interestingly, we highlighted the emergence of AppNets— large groups of tightly connected applications that promote each other. We will continue to dig deeper into this ecosystem of malicious apps on Facebook, and we hope that Facebook will benefit from our recommendations for reducing the menace on there are hackers-on-their-platform.

Future Scope: In the future, we can go with the other than text posts like image post, video post, we can classify based on the image features and video features so that we can easily detect the FB as a malicious if the user posts the unwanted images or videos.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

REFERENCES

[1] C. Pring, "100 social media statistics for 2012," 2012 [Online].
[2] R. Naraine, "Hackers selling $25 toolkit to create malicious Facebookapps," 2011 [Online].Available [Online].
[3] C.-C. Chang and C.-J. Lin, ―LIBSVM: A library for support vector machines,‖ Trans. Intell. Syst. Technol., vol. 2, no. 3, 2011, Art.no. 27.
[4] "Profile stalker: Rogue Facebook application," 2012 [Online].
[5] "Which cartoon character are you—Facebook survey scam," 2012 [Online].
[6] G. Cluley, "The Pink Facebook rogue application and survey scam," 2012 [Online].
[7] D. Goldman, "Facebook tops 900 million users," 2012 [Online].
[8] HackTrix, "Stay away from malicious Facebook apps," 2013 [Online].
[9] 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.
[10] H. Gaoet al., "Detecting and characterizing social spam campaigns," in Proc. IMC, 2010, pp. 35–47.
[11] H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary, "Towards online spam filtering in social networks," in Proc. NDSS, 2012.
[12] "WhatApp? (beta)—A Stanford Center for Internet and Society Website with support from the Rose Foundation," [Online].
[13]―MyPageKeeper,‖[Online].Available:https://www.facebook.com/pps/application.php?id= 167087893342260
[14]Facebook, Palo Alto, CA, USA, ―Application authentication flow using OAuth 2.0,‖ [Online].
[15]J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, ―Beyond blacklists: Learning to detect malicious Web sites from suspicious URLs,‖ in Proc. KDD, 2009, pp. 1245–1254.