International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Detecting Malicious Facebook Application using Digital India Scheme

M. Divya, M. Monika, N. Kanimozhi

Department of Computer Science and Engineering,
GKM College of Engineering and Technology, Chennai, Tamil Nadu, India

ABSTRACT

With 20 million installs a day third-party apps are a major reason for the popularity and addictiveness of Facebook. 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 data set are malicious. So far, the research community has focused on detecting malicious posts and campaigns. In this paper, we ask the question: given a Facebook application, can we determine if it is malicious? Our key contribution is in developing Proguard Facebook's Rigorous Application Evaluator arguably the first tool focused on detecting malicious apps on Facebook. To develop ProGuard, we use information gathered by observing the posting behavior of 111K Facebook apps seen across 2.2 million users on Facebook. First, we identify a set of features that help us distinguish malicious apps from benign ones.For example, we find that malicious apps often share names with other apps, and they typically request fewer permissions than benign apps. Second, leveraging these distinguishing features, we show that ProGuard can detect malicious apps with 100% accuracy, with no false positives and a low false negative rate (4.1%). Finally, we explore the ecosystem of malicious Facebook apps and identify mechanisms that these apps use to propagate. Interestingly, we find that many apps collude and support each other; in our dataset, we find 1,584 apps enabling the viral propagation of 3,723 other apps through their posts. Long-term, we see ProGuard as a step towards creating an independent watchdog for app assessment and ranking, so as to warn Facebook users before installing apps And improved online infrastructure and by increasing Internet connectivity so that we can avoid fraud and cheating.

Keywords: *Proguard, Online social Network, Security, Malicious Account, Aadhar Number, OTP*

I. Introduction

Online social networks (OSN) enable and encourage third party applications (apps) to enhance the user experience on these plat-forms. 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 Face-book and on average, 20M apps are installed every day. 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 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, and (c) the app can "re-produce" by making other malicious apps popular. Virtual currencies are becoming standard offering for online games sites, social media sites and other business. Virtual currency systems generate revenue provides low cost alternative to credit cards for micropayments, offer prepaid solutions and other users without credit cards

and help companies built alternative loyalty program. In addition, complex virtual currency and virtual wallet programs involve more complex privacy and security issues such as joint ownership or sharing of customer information. Virtual currency security can be implemented using digital india scheme by sending one-time password to gmail.

II. Related Works

An Joshua s.Gans and Hanna Halaburda, proposed a method to increase the activity of users in facebook. Limiting functionality and allowing for both "buying" and "earning" are features that maximize activity on the platform. Users spend Facebook credits to enhance their paltform experience, which increases their utility from using the platform and leads to more activity(2013). Asaf Shabatai, Uri kanonov, Yuval Elovic introduced a configuration manager manages the configuration of application. The Alert Handler triggers an action as a result of dispatched alert. The prossecor manager register / unregister processor, and activities / deactivities the processor (2011). Mark Rose, Rajiv dutta, Lex N. Bayer developed the Virtual Currency Configuration apparatus, method and system(VCC) transform request for ondemand and flexible monetization and related services via VCC components into currency transfers, purchase receipt notifications, social networking communications and transaction analytics reports(2012).

III. Proposed System

In order to effectively detect malicious accounts in online promotion activities by overcoming the aforementioned challenges, we have designed a novel system, namely ProGuard. ProGuard employs a collection of behavioral features to profile an account that participates in an online promotion event. These features aim to characterize an account from three aspects including

i) Its general usage profile

ii) How an account collects virtual currency

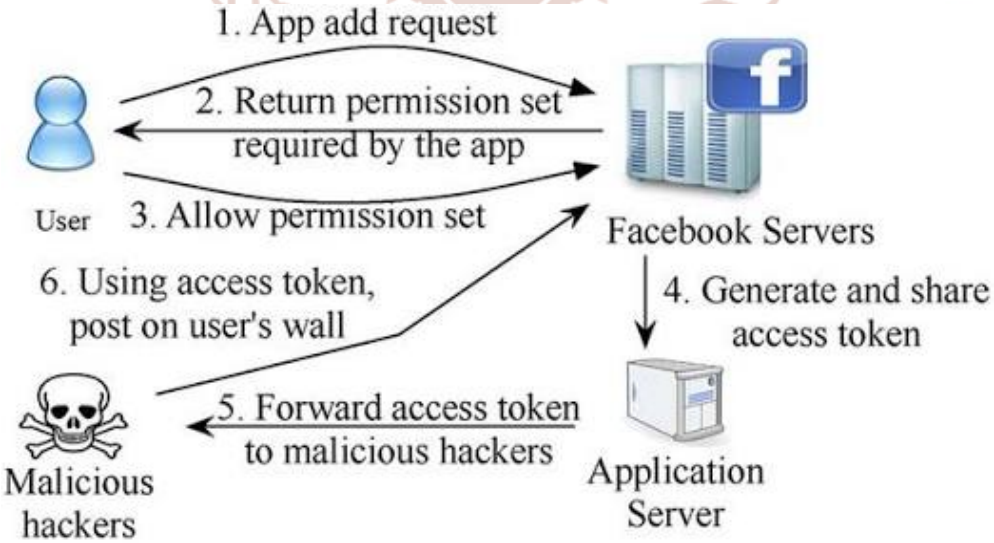
iii) How the virtual currency is spent.

iv) Sending One-Time Password to G-Mail id.

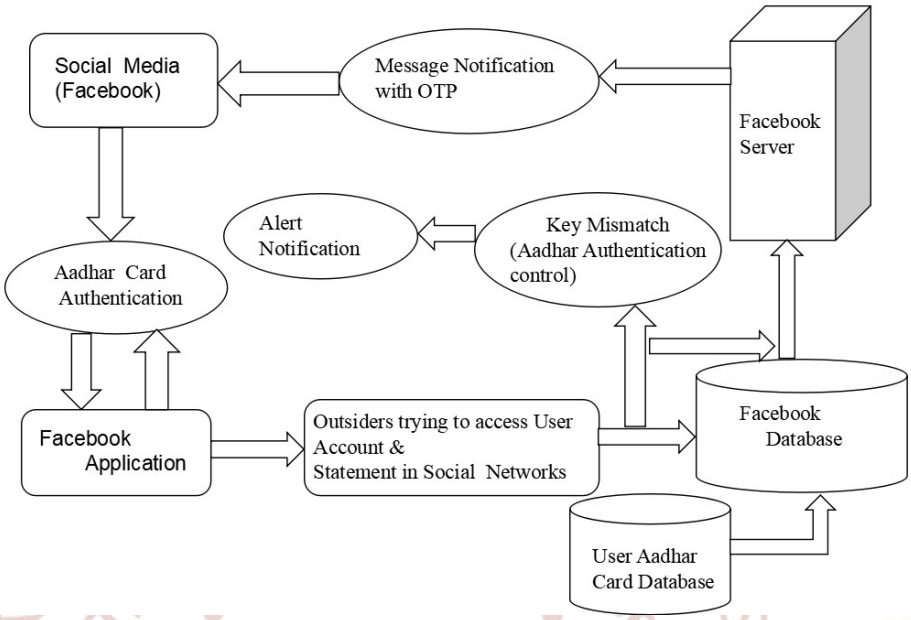
ProGuard further integrates these features using a statistical classifier so that they can be collectively used to discriminate between those accounts controlled by attackers and benign ones. To the best of our knowledge, this work represents the first effort to systematically detect malicious accounts used for online promotion activity participation. We have evaluated our system using data collected from Tencent QQ, a leading Chinese online social network that uses a widely-accepted virtual currency (i.e., Q coin), to support online financial activities for a giant body of 899 million active accounts.

Our experimental results have demonstrated that ProGuard can achieve a high detection rate of 100% with a very low false positive rate of 0.3% after using digital India scheme.

SYSTEM MODEL:



SYSTEM ARICHTECTURE:



A. AUTHENTICATION MODULE:

In this module, Owner Activate the number of Users. Number of Users is controlled by only Owner. In this method user can have more than account. This module describes the authentication so Owner and Users enters the application through login. Owner and Users must have the separate username password.

B. IMAGE UPLOAD AND UPDATE:

In this module number of users uploads the image into the facebook, with the help of this metadata and its contents. In this module user can update user profile into facebook. And also we are updating personal details along with the picture.

C. VIEW REQUEST:

In this module user can view all the friend request and also make the unfollow and also we can see the user profile. We can accept the friend requests that are not in our friend list.

D. ONLINE SHOPPING:

In this module we can access the virtual currency from online social networks and spent the amount in online shopping. By generating the One-Time Password through G-mail address further purchasing process to be proceed.

E. CONCULSIONS:

This paper presents a novel system, ProGuard, to automatically detect malicious OSN accounts that participate in online promotion events. ProGuard leverages three categories of features including general behavior, virtual-currency collection, and virtual-currency usage. Experimental results based on labelled data collected from Tencent QQ, a global leading OSN company, have demonstrated the detection accuracy of ProGuard, which has achieved a high detection rate of 100% given an extremely low false positive rate of 0.3% using digital India scheme.

REFERENCES

1. Y. Wang and S. D. Mainwaring, "Human-currency interaction: learning from virtual currency use in china," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2008, pp. 25–28.
2. Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia, "Detecting automation of twitter accounts: Are you a human, bot, or cyborg?" IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 6, pp. 811–824, 2012.
3. Z. Chu, S. Gianvecchio, A. Koehl, H. Wang, and S. Jajodia, "Blog or block: Detecting blog bots through behavioral biometrics," Computer Networks, vol. 57, no. 3, pp. 634–646, 2013.

4. J. S. Gans and H. Halaburda, "Some economics of private digital currency," Rotman School of Management Working Paper, no. 2297296, 2013.
5. X. Hu, J. Tang, and H. Liu, "Online social spammer detection," in Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence. AAAI, 2014, pp. 59–65.
6. "Leveraging knowledge across media for spammer detection in microblogging," in Proceedings of the 37th international ACM SIGIR conference on Research & development in information retrieval. ACM, 2014, pp. 547–556.
7. S. Fakhraei, J. Foulds, M. Shashanka, and L. Getoor, "Collective spammer detection in evolving multi-relational social networks," in Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 2015, pp. 1769–1778.