Identifying New Malicious Detecting Application

R. Pitchandi[1], M. Deepika[2]

[1]*Associate Professor,* [2]*Final Year MCA Student*

Department of Computer Applications, Madha Engineering College, Chennai, India

Abstract - The solution is already find as we significant that at least of apps in our dataset are malicious third-party apps area major reason. Online social media service, people now have accounts on multiple and diverse services like facebook twitter and YouTube. To develop FRAppE - Facebook's Rigorous Application Evaluator, we use information gathered by observing the posting behavior of thousands FRAppE apps seen across 2.2 million users on facebook. Public used user ID, display name, illustration, position, profile picture, and number of connections to generate the user. Classifiers for disambiguating profile belonging to the same user from different social network. We explore the ecosystem of malicious FRAppE apps and particular mechanisms that these apps use to propagate. Interestingly, we find that many apps collude and support in our dataset we see facebook apps as a step toward creating an independent watchdog for application assessment and ranking, so as to warn Facebook users before installing a FRAppE applications.

Keywords: FRAppE, detecting apps, malicious social network

I. INTRODUCTION

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 [2] that facilitates app integration into the Facebook user experience. There are 500K apps available on Facebook [3], and on average, 20M apps are installed every day [1]. Furthermore, many applications have acquired and maintain a really large user base. For instance, Farmville and City Ville apps have 26.5Mand 42.8M users to date. Recently, hackers have started taking advantage of the popularity of this third-party application platform and deploying malicious applications. Malicious applications 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:

1) The application can reach large numbers of users and their friends to spread spam.

2) The application can obtain users' personal information such as e-mail address, home town.

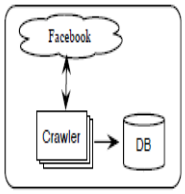
3) The application can "reproduce" by making other malicious applications popular.

To make matters worse, the deployment of malicious apps is simplified by ready-to-use toolkits starting at $25 [8]. In other words, there is motive and opportunity, and as a result, there are many malicious apps spreading on Facebook every day [9].Despite the above worrisome trends, today a user has very limited information at the time of installing an application on Facebook. 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 application.

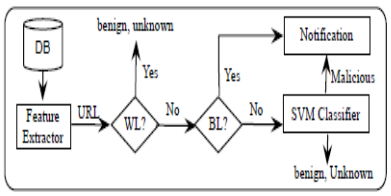
As we show in Section III, malicious applications are widespread and they easily spread, as an infected user jeopardizes the safety of all its friends'. So far, the research community has paid little attention to OSN apps specifically. Most research related to spam and malware on Facebook has focused on detecting malicious posts and social spam campaigns [10]–[12]. At the same time,

in a seemingly backwards step, Facebook has dismantled its application rating functionality recently. A recent work studies how application permissions and community ratings correlate to privacy risks of Facebook apps [13]. Finally, there are some community-based feedback-driven efforts to rank applications, such as What Application? [14]; though these could be very powerful in the future, so far they have received little adoption. We discuss previous work in more detail in Section VIII. In this paper, 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 [15] that monitors the Facebook profiles of 2.2 million users. We analyze 111K applications that made 91 million posts over 9 months. This is arguably the first comprehensive study focusing on malicious Facebook applications that focuses on quantifying, profiling, and understanding malicious applications and synthesizes this information into an

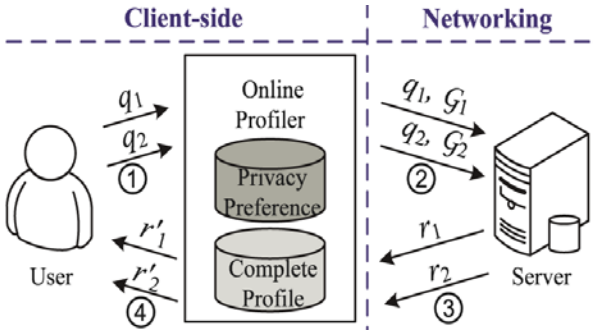
effective detection approach. Our work makes the following key contributions

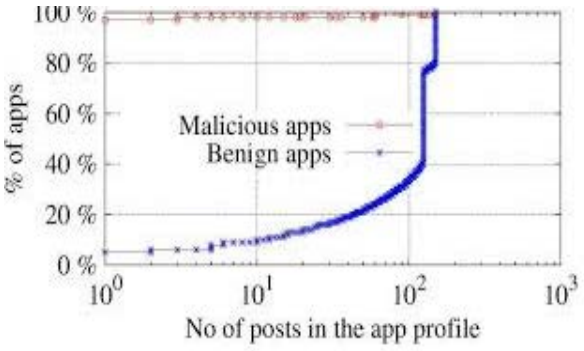


Crawling Facebook posts



Classifying Facebook posts





13% of observed apps are malicious. We show that malicious applications are prevalent in Facebook and each a large number of user's. We find that 13% of applications in our dataset of111K distinct apps are malicious. Also, 60% of malicious applications endanger more than 100K users each by convincing them to follow the links on the posts made by these apps, and 40% of malicious apps have over 1000 monthly active users each.

Malicious and benign application profiles significantly differ. We systematically profile applications and show that malicious application profiles are significantly different than those of benign applications. A striking observation is the "laziness" of hackers, many malicious apps have the same name, as 8%of unique names of malicious apps are each used by more than10 different apps (as defined by their application IDs). Overall, we profile apps based on two classes of features:

1) Those that can be obtained on-demand given an application's identifier (e.g., the permissions required by the app and the posts in the application's profile page), and

2) Others that require a cross-user view to aggregate information across time and across apps (e.g., the posting behavior of the app and the similarity of its name to other apps).

The emergence of app-nets: Apps collude at massive scale. We conduct a forensics investigation on the malicious application system to identify and quantify the techniques used to promote malicious applications. We find that apps collude and collaborate at a massive scale. Apps promote other apps via posts that point to the "promoted" apps. If we describe the collusion relationship of promoting–promoted apps as a graph, we find 1584 promoter apps that promote 3723 other applications. Furthermore, these apps form large and highly dense connected components, as shown in Fig. 1.Furthermore, hackers use fast-changing indirection: Applications posts have URLs that point to a Web site, and the Web site dynamically redirects to many different apps; we

Find 103 such URLs that point to 4676 different malicious applications over the course of a month. These observed behaviors indicate well-organized crime: One hacker controls many malicious apps, which we will call an app-net, since they seem a parallel concept to bonnets .Malicious hackers impersonate applications. We were surprised to find popular good apps, such as Farmville and Facebook for iPhone, posting malicious posts. On further investigation, we found a lax authentication rule in Facebook that enabled hackers to make malicious posts appear as though they came from these apps.

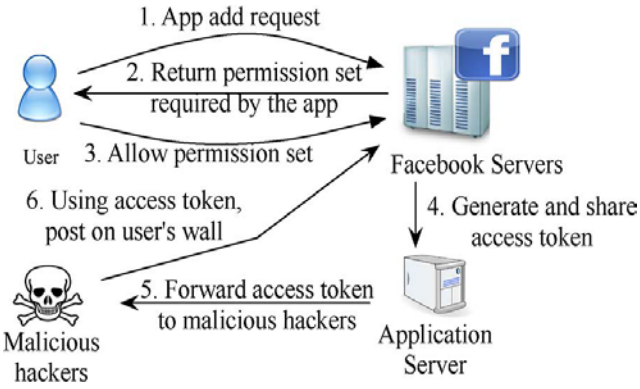
FRAppE can detect malicious apps with 99% accuracy. We develop FRAppE (Facebook's Rigorous Application Evaluator) to identify malicious apps using either using only features that can be obtained on-demand or using both on-demand and aggregation-based app information.

FRAppE Lite, which only uses information available on-demand, can identify malicious apps with 99.0%accuracy, with low false positives (0.1%) and high true positives (95.6%). By adding aggregation-based information, Frappe can detect malicious apps with 99.5%accuracy, with no false positives and higher true positives(95.9%).

II. SYSTEM MODEL

Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy

concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing.



III. PREVIOUS WORK

Detecting Spam on OSNs: analyzed posts on the walls of 3.5 million Facebook users and showed that10% of links posted on Facebook walls are spam. They also presented techniques to identify compromised accounts and spam campaigns. Develop efficient techniques for online spam filtering on OSNs such as Facebook .rely on having the whole social graph as input, and so is usable only by the OSN provider. Develop a third-party application for spam detection on Facebook. Others present mechanisms for detection of spam URLs on Twitter. In contrast to all of these efforts, rather than classifying individual URLs or posts as spam, we focus on identifying malicious applications that are the main source of spam on Facebook. . Detecting Spam Accounts: developed techniques to identify accounts of spammers on Twitter. Others have proposed a honey-pot-based approach to detect spam account son OSNs .analyzed behavioral patterns among spam accounts in Twitter. Instead of focusing on account secreted by spammers, our work enables detection of malicious apps that propagate spam and malware by luring normal users to install them. Use a real application named “Photo of the Day” to demonstrate how malicious app son Facebook can launch distributed denial-of-service (DDoS) attacks using the Facebook platform. Conducted survey to understand users’ interaction with Facebook apps. Similarly, study the user reach of popular Facebook applications. On the contrary, we quantify the prevalence of malicious apps and develop tools to identify malicious apps that use several features beyond the required permission set.

IV. PROPOSED METHODOLOGY

13% of observed applications are malicious. We show that malicious applications are prevalent in Facebook and reach a large number of users. We find that 13% of apps in our dataset of111K distinct applications are malicious. Also, 60% of malicious apps endanger more than 100K users each by convincing them to follow the links on the posts made by these applications, and 40% of malicious apps have over 1000 monthly active users each. Malicious and benign app profiles significantly differ. We systematically profile apps and show that malicious approve files are significantly different than those of benign apps. A striking observation is the “laziness” of hackers; many malicious apps have the same name, as 8%of unique names of malicious apps are each used by more than10 different applications (as defined by their application IDs). Overall, we profile apps based on two classes of features

V. PROPOSED SYSTEM FEATURES

1. Those that can be obtained on-demand given an application’s identifier (e.g., the permissions required by the app and the posts in the application’s profile page).

2. Others that require a cross-user view to aggregate information across time and across apps (e.g. the posting behavior of the application and the similarity of its name to other applications)

Apps promote other apps via posts that point to the “promoted” applications. If we describe the collusion relationship of promoting–promoted applications as a graph, we find 1584 promoter applications that promote 3723 other applications. Malicious hackers impersonate applications. We were surprised to find popular good apps, such as Farm Ville and Facebook for iPhone, posting malicious posts. On further investigation, we found a lax authentication rule in Facebook that enabled hackers to make malicious posts appear as though they came from these apps.

FRAppE can detect malicious apps with 99% accuracy. We develop FRAppE (Facebook’s Rigorous Application Evaluator) to identify malicious applications using either using only features that can be obtained on-demand or using both on-demand and aggregation-based application information. FRAppE Lite, which only uses information available on-demand, can identify malicious apps with 99.0%accuracy, with low false positives (0.1%) and high true positives (95.6%). By adding aggregation-based information, FRAppE can detect malicious applications with 99.5%accuracy, with no false positives and higher true positives (95.9%). The proposed work is arguably the first comprehensive study focusing on malicious Facebook applications that focuses on quantifying, profiling, and understanding malicious apps and synthesizes this information into an effective detection approach. Several features used by FRAppE, such as the reputation of redirect URIs, the number of required permissions, and the use of different client IDs in app installation URLs, are

robust to the evolution of hackers. Not using different client IDs in application installation URLs would limit the ability of hackers to instrument their applications to propagate each other

VI. CONCLUSION

In this paper, we proposed a simple and generic method to convert any ABE scheme with non-verifiable outsourced decryption to an ABE scheme with verifiable outsourced decryption in the standard model. To concretely assess the performance of the new method, we presented an instantiation of our generic method based on Green etal.'soutsourced-ABEscheme without verifiability. We implemented our instantiation, Green et al.'s scheme. Verifiable outsourced scheme on PC. Experiment results showed that our method is nearly optimal in the sense that it introduces minimal overhead in exchange for verifiability.

REFERENCES

[1] D.Irani, S. Webb, K. Li, and C.Pu, "Large online social footprints-an Emerging threat," in *CSE* '09, vol. 3, aug. 2009, pp. 271-276

[2] R.Zafarani and H.Liu,"Connecting corresponding identities across communities," 2009. [online].

[3] M.Rowe and F. Ciravegna, "Harnessing the social web: The science of identity disambiguation," in *Web Science Conference*, 2010.

[4] C.Priya, "100 social media statistics for 2012,"2012[online]. Available:http://thesocialskinny.com/100-social-media-statistics-for-2012/

[5] "Wiki: Facebook platform," 2014 [online].Available: http//en.wikipedia.org/wiki/facebook_Platform

[6] D. Goldman, :Facebook tops 900 million users," 2012 [online]. Available:

[7] H. Gao et al., "Detecting and characterizing social spam campaigns,"In Proc.*IMC*, 2010,pp. 35_47.

[8] Facebook, Palo Alto, CA, USA, :Facebook platform policies."[online]. Available:

[9] "11 million bulk email address for sale-Sale price $90."[online]. Available:http://www.allhomebased.com/BulkEmailAddresses.htm

[10] T. Stein, E. Chen, and K. Mangla, "Facebook immune system,"in Proc 4th Workshop Social Netw,Syst.,2011,Art.no.8.