ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Segmenting and Detecting Malicious Tweets and Harmful Entity Recognition

G. Saranya[1], D. Michael Kamaraj[2]

Research Scholar, Department of Computer Science, Sudharsan College of Arts and Science, Perumanadu, Pudukkottai District, Tamil Nadu, India.

Asst. Professor, Department of Computer Science, Sudharsan College of Arts and Science, Perumanadu, Pudukkottai District, Tamil Nadu, India.

ABSTRACT: Social Network has attracted millions of users to share and disseminate most up-to-date information, resulting in large volumes of data produced every day. The main objective of the today's modern social networking world is to provide online safety through automatic monitoring of Cyberbullying and watchdog in the social networking sites. The existing system focuses on automatic monitoring of Cyberbullying but lacks an effective prevention and follow-up strategy. FRAppE—Facebook's Rigorous Application Evaluator finds the optimal segmentation of a data by maximizing the sum of the stickiness scores of its candidate segments. The stickiness score considers the probability of a segment being a phrase in English (i.e., global context) and the probability of a segment being a phrase within the batch of tweets (i.e., local context). The major contribution of this approach is a research agenda for a social networking application pursuing the aim to detect the above mentioned threats to improve the situation.

KEYWORDS: Social Network, Security, Protection, Access controls, Verification.

I. INTRODUCTION

Online social networks (OSN) 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 large user base. For instance, FarmVille and CityVille 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 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.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

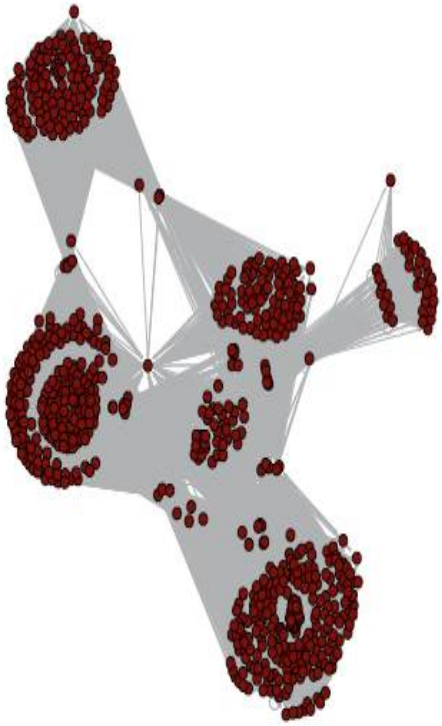


Figure 1: The emergence of AppNets on Facebook. Real snapshot of 770 highly collaborating apps: an edge between two apps means that one app helped the other propagate. Average degree (no. of collaborations) is 195!

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.

II. CONTRIBUTIONS OF THE SYSTEM

13% of the observed apps are malicious. We show that malicious apps are prevalent in Facebook and reach a large number of users. We find that 13% of apps in our dataset of 111K distinct apps 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 apps, and 40% of malicious apps have over 1,000 monthly active users each.

Malicious and benign app profiles significantly differ. We systematically profile apps and show that malicious app profiles 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 than 10 different apps (as defined by their app IDs). Overall, we profile apps based on two classes of features: (a) 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 (b) 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).

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

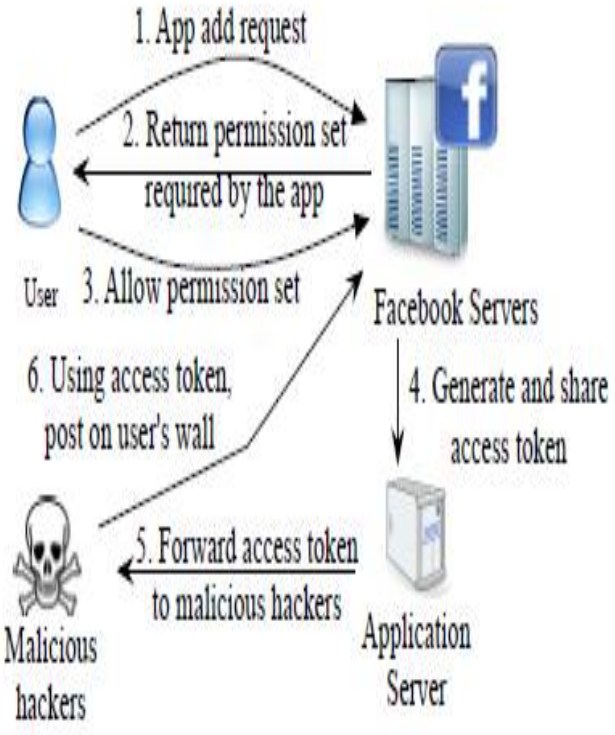


Figure 2: Steps involved in hackers using malicious applications to get access tokens to post malicious content on victims' walls.

The emergence of AppNets: apps collude at massive scale. We conduct a forensics investigation on the malicious app ecosystem to identify and quantify the techniques used to promote malicious apps. The most interesting result is that apps collude and collaborate at a massive scale.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

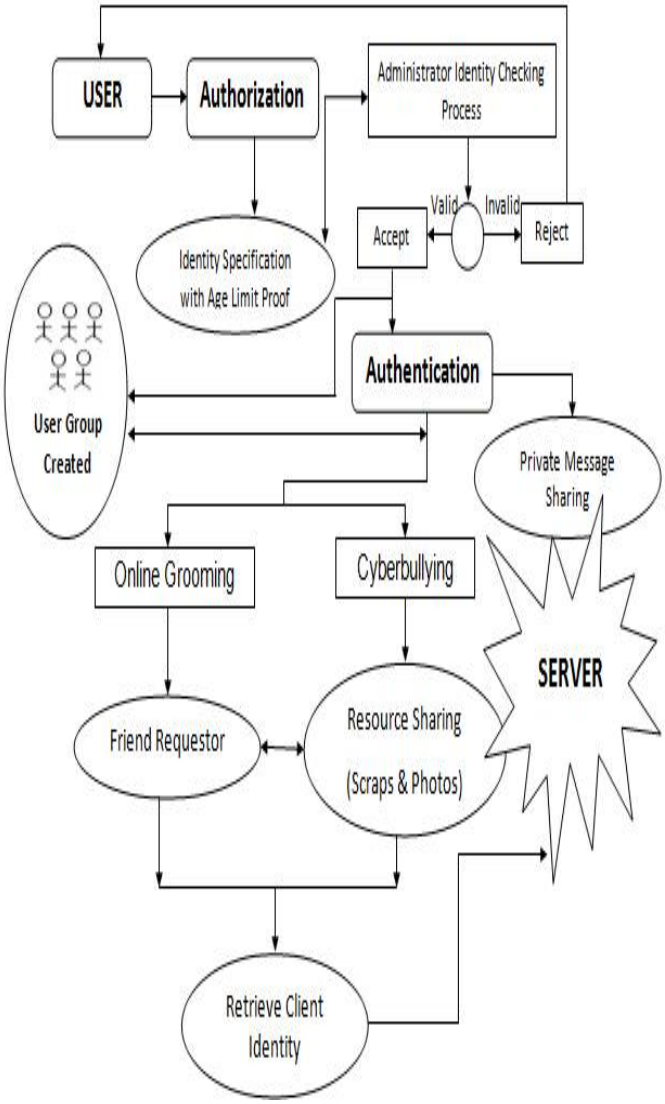


Figure.3. System Architecture Design

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 1,584 promoter apps that promote 3,723 other apps. 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 website, and the website dynamically redirects to many different apps; we find 103 such URLs that point to 4,676 different malicious apps over the course of a month. These observed behaviors indicate well-organized crime: one hacker controls many malicious apps, which we will call an AppNet, since they seem a parallel concept to botnets.

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 either using only features that can be obtained on-demand or using both on-demand and aggregationbased app information. FRAppE Lite, which only uses information available on-

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

demand, can identify malicious apps with 99.0% accuracy, with low false positives (0.1%) and false negatives (4.4%). By adding aggregation-based information, FRAppE can detect malicious apps with 99.5% accuracy, with no false positives and lower false negatives (4.1%).

III. PROPOSED CONTRIBUTIONS

In this system, we focus on the task of tweet/scrap segmentation. The goal of this task is to split a tweet into a sequence of consecutive n-grams (n<=1), each of which is called a segment. To achieve high quality tweet segmentation, we propose a generic tweet/scrap segmentation framework, named FRAppE—Facebook's Rigorous Application Evaluator. FRAppE learns from both global and local contexts, and has the ability of learning from pseudo feedback. A segment can be a named entity, a semantically meaningful information unit (e.g., "officially released"), or any other types of phrases which appear "more than by chance". Recommendation system is proposed in order to detect the misuses involved in cyber bulling as well as by means of effective authentication means. Automatic warnings before uploading of critical and harmful messages. Automatic forwarding of harmful texts to the trustee based on severity of the text, which is already updated by the message auditor into the server end.

Advantages:

- Proposed system provides automatic warnings before uploading critical and harmful messages.
- Follow-up strategies focus on preventing future cyberbullying and empowering the user with the help of trusted contacts.
- Verifying the age proof before allows the user to registering into the system.
- Watchdog mechanism is included into the proposed approach.

FACEBOOK APPS

Facebook enables third-party developers to offer services to its users by means of Facebook applications. Unlike typical desktop and smartphone applications, installation of a Facebook application by a user does not involve the user downloading and executing an application binary. Instead, when a user adds a Facebook application to her profile, the user grants the application server: (a) permission to access a subset of the information listed on the user's Facebook profile (e.g., the user's email address), and (b) permission to perform certain actions on behalf of the user (e.g., the ability to post on the user's wall). Facebook grants these permissions to any application by handing an OAuth 2.0 token to the application server for each user who installs the application. Thereafter, the application can access the data and perform the explicitly-permitted actions on behalf of the user. Fig. 2 depicts the steps involved in the installation and operation of a Facebook application.

MYPAGEKEEPER

MyPageKeeper is a Facebook app designed for detecting malicious posts on Facebook. Once a Facebook user installs My-PageKeeper, it periodically crawls posts from the user's wall and news feed. MyPageKeeper then applies URL blacklists as well as custom classification techniques to identify malicious posts. Our previous work shows that MyPageKeeper detects malicious posts with high accuracy—97% of posts flagged by it indeed point to malicious websites and it incorrectly flags only 0.005% of benign posts.

The key thing to note here is that MyPageKeeper identifies social malware at the granularity of individual posts, without grouping together posts made by any given application. In other words, for every post that it crawls from the wall or news feed of a subscribed user, MyPageKeeper's determination of whether to flag that post does not take into account the application responsible for the post. Indeed, a large fraction of posts (37%) monitored by MyPage-Keeper are not posted by any application; many posts are made manually by a user or posted via a social plugin (e.g., by a user clicking 'Like' or 'Share' on an external website). Even among malicious posts identified by MyPageKeeper, 27% do not have an associated application.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

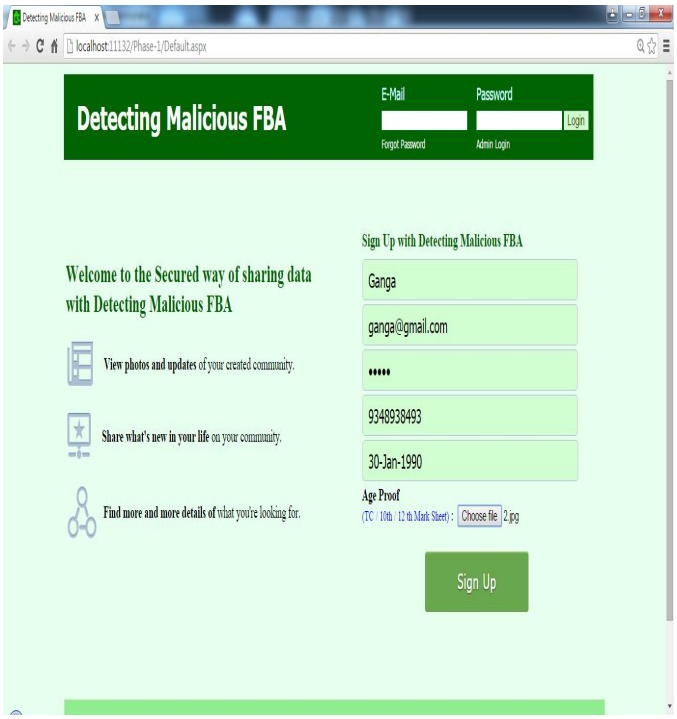
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

MyPageKeeper's classification primarily relies on a Support Vector Machine (SVM) based classifier that evaluates every URL by combining information obtained from all posts containing that URL. Examples of features used in MyPageKeeper's classifier include a) the presence of spam keywords such as 'FREE', 'Deal', and 'Hurry' (malicious posts are more likely to include such keywords than normal posts), b) the similarity of text messages (posts in a spam campaign tend to have similar text messages across posts containing the same URL), and c) the number of 'Like's and comments (malicious posts receive fewer 'Like's and comments). Once a URL is identified as malicious, MyPageKeeper marks all posts containing the URL as malicious.

Experimental Results

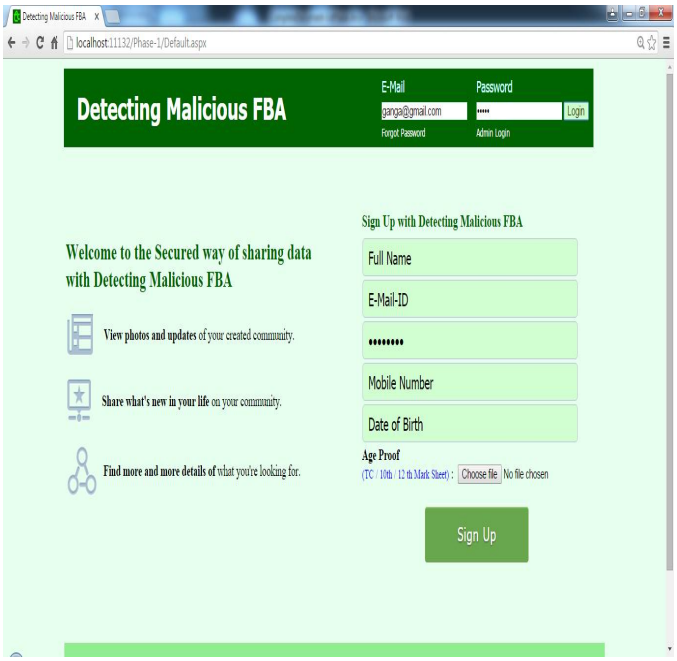


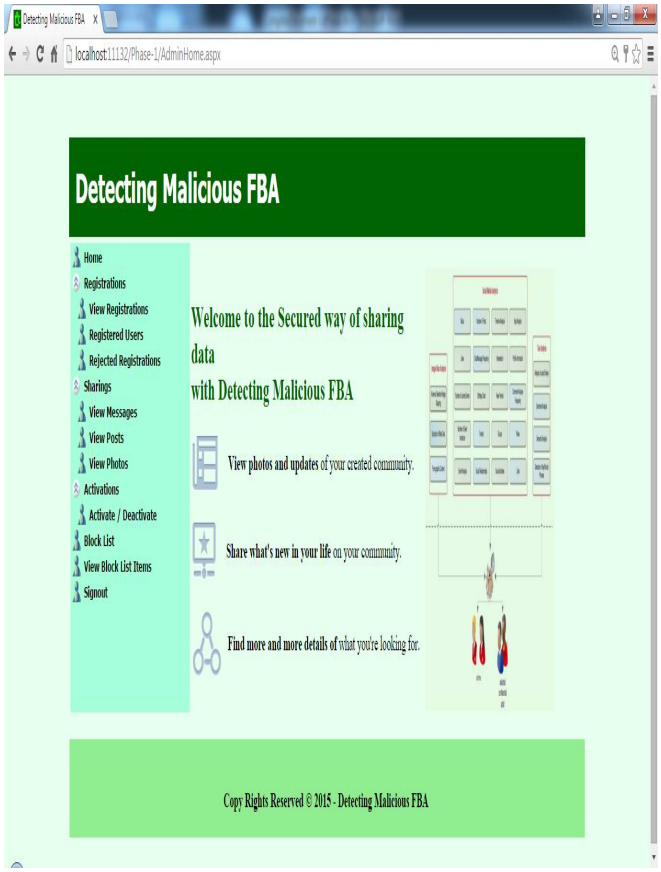
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016



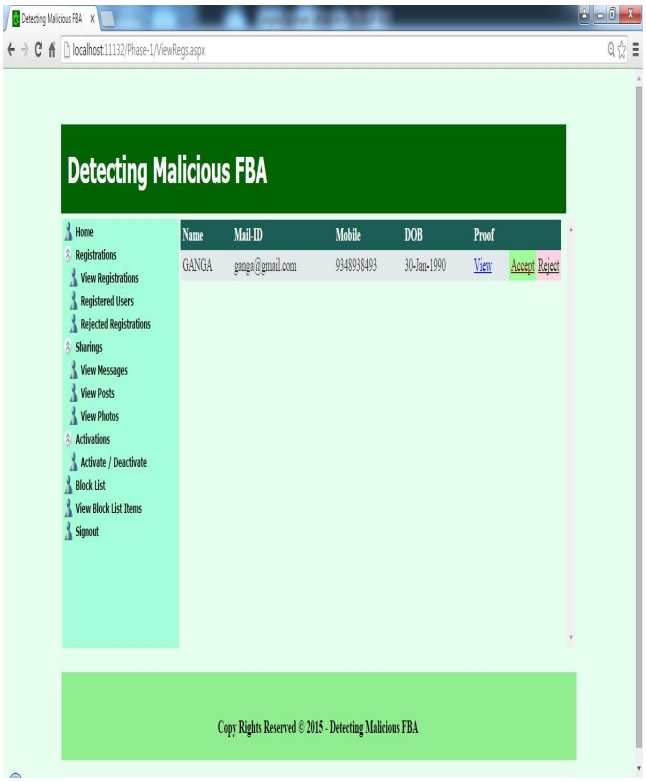


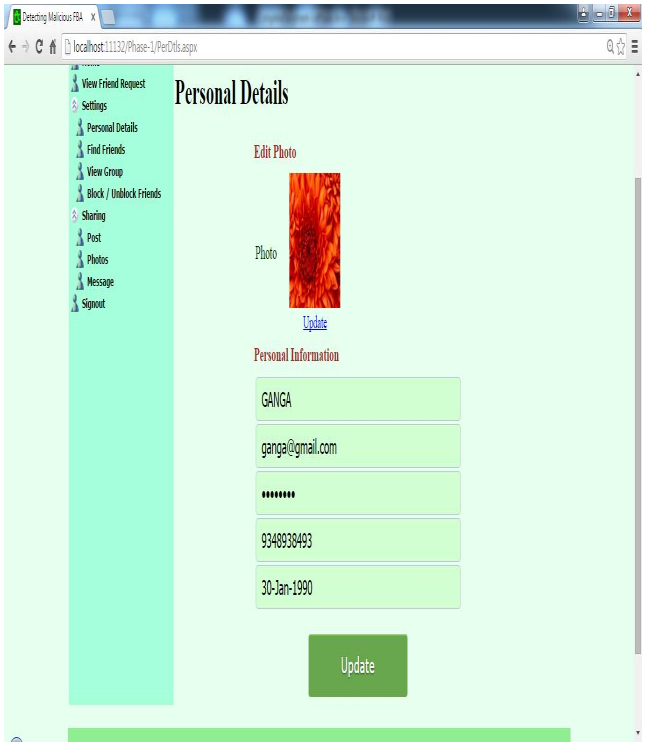
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016





ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

IV. CONCLUSION AND FUTURE WORK

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 fewer permissions than benign apps. Leveraging our observations, we developed FRAppE, 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 of hackers on their platform.

REFERENCES

[1] A. Besmer, H. R. Lipford, M. Shehab, and G. Cheek. Social applications: exploring a more secure framework. In SOUPS, 2009.
[2] C.-C. Chang and C.-J. Lin. LIBSVM: A library for support vector machines. ACM Transactions on Intelligent Systems and Technology, 2, 2011.
[3] P. Chia, Y. Yamamoto, and N. Asokan. Is this app safe? a large scale study on application permissions and risk signals. In WWW, 2012.
[4] F. J. Damerau. A technique for computer detection and correction of spelling errors. Commun. ACM, 7(3), Mar. 1964.
[5] H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary. Towards online spam filtering in social networks. In NDSS, 2012.
[6] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao. Detecting and characterizing social spam campaigns. In IMC, 2010.
[7] M. Gjoka, M. Sirivianos, A. Markopoulou, and X. Yang. Poking facebook: characterization of osn applications. In Proceedings of the first workshop on Online social networks, WOSN, 2008.
[8] J. King, A. Lampinen, and A. Smolen. Privacy: Is there an app for that? In SOUPS, 2011.
[9] Facebook kills App Directory, wants users to search for apps. http://zd.net/MkBY9k.
[10] Facebook Opengraph API. http://developers.facebook.com/docs/reference/api/.
[11] Facebook softens its app spam controls, introduces better tools for developers. http://bit.ly/LLmZpM.
[12] Facebook tops 900 million users. http://money.cnn.com/2012/04/23/technology/facebook-q1/index.htm.
[13] Hackers selling $25 toolkit to create malicious Facebook apps. http://zd.net/g28HxI.
[14] MyPageKeeper. https://www.facebook.com/apps/application.php?id=167087893342260.
[15] Norton Safe Web. http://www.facebook.com/apps/application.php?id=310877173418.
[16] Permissions Reference. https://developers.facebook.com/docs/authentication/permissions/.
[17] Pr0file stalker: rogue Facebook application. https://apps.facebook.com/mypagekeeper/?status=scam_report_fb_survey_scam_pr0file_viewer_2012_4_4.
[18] Selenium - Web Browser Automation. http://seleniumhq.org/.
[19] SocialBakers: The receipe for social marketing success. http://www.socialbakers.com/.
[20] Stay Away From Malicious Facebook Apps. http://bit.ly/b6gWn5.
[21] The Pink Facebook - rogue application and survey scam. http://nakedsecurity.sophos.com/2012/02/27/pink-facebook-survey-scam/.
[22] Web-of-trust. http://www.mywot.com/.