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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

Detection of Behavioral Anomaly of Compromised Accounts in OSN's

K.Maheswara Reddy[1] , A.L.Sreenivasulu [2]

M.Tech Student, Dept. of CSE, GATES Engineering College, Affiliated to JNTUA, Andhra Pradesh, India [1]

Associate Professor & HOD, Dept. of CSE, GATES Engineering College, Affiliated to JNTUA,

Andhra Pradesh, India[2]

ABSTRACT: A social behavioral profile accurately reflects a user's OSN activity patterns. People access OSNs using both traditional desktop PCs and new emerging mobile devices. With more than one billion users worldwide, OSNs are a new venue of innovation with many challenging research problems. In this paper, we study the social behaviors of OSN users, i.e., their usage of OSN services, and the application of which in detecting the compromised accounts. We capture user behavior with the following metrics: user connectivity, user activity and user reactions. we validate and characterize the user social activity on OSN. The study is based on detailed clickstream data ,the clickstream data reveals key features of the social network workloads, such as how frequently people connect to social networks and for how long, as well as the types and sequences of activities that users conduct on these sites. we pay attention to the characteristics of social behaviors we review malicious behaviors of OSN users and show the social behavioral profiles can accurately differentiate individual OSN users and detect compromised accounts.

KEYWORDS: Online social behavior, privacy, data analysis, compromised accounts detection.

I.INTRODUCTION

Online social networks (OSNs) have become extremely popular.Social media have pulled ahead of email as the most popular online activity. More than two-thirds of the global online population visit and participate in social networks and blogs. In fact, social networking and blogging account for nearly 10% of all time spent on the Internet. These statistics suggest that OSNs have become a fundamental part of the global online experience. OSN user behavior covers various social activities that users can do online, such as friendship creation, content publishing, profile browsing, messaging, and commenting. Notably, these activities can be legitimate or malicious. Understanding how users behave when they connect to these sites is important for a number of reasons because these days compromised accounts are targeted or we can say preferred by spammers. The malicious one breaks the trust relationships between the legitimate account owners and their friends, and efficiently distribute spam ads, phishing links, or malware.

Now a day's hacking someone's online social networking profiling attributes and then usage of the same for any vulgar activities is been a serious threat. The account of celebrities or political leaders is mostly bait for this kind of system. Many systems are been proposed to identify this kind of profiling attack but most of them are relay on observed facts about the accounting which generally takes longer time to identify the attack. So to diminish this time of detection for early stages of the compromised attacks system should have capable of detection of hidden states. This idea eventually increases the early detection which can avoid serious threats

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

II. LITERATURE SURVEY

Y. Bachrach, M. Kosinski, T. Graepel, P. Kohli, and D. Stillwell

We show how users' activity on Facebook relates to their personality, as measured by the standard Five Factor Model. Our dataset consists of the personality profiles and Facebook profile data of 180,000 users. We examine correlations between users' personality and the properties of their Facebook profiles such as the size and density of their friendship network, number uploaded photos, number of events attended, number of group memberships, and number of times user has been tagged in photos. Our results show significant relationships between personality traits and various features of Facebook profiles. We then show how multivariate regression allows prediction of the personality traits of an individual user given their Facebook profile. The best accuracy of such predictions is achieved for Extraversion and Neuroticism, the lowest accuracy is obtained for Agreeableness, with Openness and Conscientiousness lying in the middle.

F. Benevenuto, T. Rodrigues, M. Cha, and V. Almeida

Understanding how users behave when they connect to social networking sites creates opportunities for better interface design, richer studies of social interactions, and improved design of content distribution systems. In this paper, we present a first of a kind analysis of user workloads in online social networks. Our study is based on detailed clickstream data, collected over a 12-day period, summarizing HTTP sessions of 37,024 users who accessed four popular social networks: Orkut, MySpace, Hi5, and LinkedIn. The data were collected from a social network aggregator website in Brazil, which enables users to connect to multiple social networks with a single authentication. Our analysis of the clickstream data reveals key features of the social network workloads, such as how frequently people connect to social networks and for how long, as well as the types and sequences of activities that users conduct on these sites. Additionally, we crawled the social network topology of Orkut, so that we could analyze user interaction data in light of the social graph. Our data analysis suggests insights into how users interact with friends in Orkut, such as how frequently users visit their friends' or non-immediate friends' pages. In summary, our analysis demonstrates the power of using clickstream data in identifying patterns in social network workloads and social interactions. Our analysis shows that browsing, which cannot be inferred from crawling publicly available data, accounts for 92% of all user activities. Consequently, compared to using only crawled data, considering silent interactions like browsing friends' pages increases the measured level of interaction among users.

H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary

Online social networks (OSNs) are extremely popular among Internet users. Unfortunately, in the wrong hands, they are also effective tools for executing spam campaigns. In this paper, we present an online spam filtering system that can be deployed as a component of the OSN platform to inspect messages generated by users in real-time. We propose to reconstruct spam messages into campaigns for classification rather than examine them individually. Although campaign identification has been used for offline spam analysis, we apply this technique to aid the online spam detection problem with sufficiently low overhead. Accordingly, our system adopts a set of novel features that effectively distinguish spam campaigns. It drops messages classified as “spam” before they reach the intended recipients, thus protecting them from various kinds of fraud. We evaluate the system using 187 million wall posts collected from Facebook and 17 million tweets collected from Twitter. In different parameter settings, the true positive rate reaches 80.9% while the false positive rate reaches 0.19% in the best case. In addition, it stays accurate for more than 9 months after the initial training phase. Once deployed, it can constantly secure the OSNs without the need for frequent re-training. Finally, tested on a server machine with eight cores (Xeon E5520 2.2Ghz) and 16GB memory, the system achieves an average throughput of 1580 messages/sec and an average processing latency of 21.5ms on the Facebook dataset.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

III. EXISTING SYSTEM

Previous research on spamming account detection mostly cannot distinguish compromised accounts from sybil accounts, with only one recent study by Egele et al. features compromised accounts detection.

Existing approaches involve account profile analysis and message content analysis (e.g. embedded URL analysis and message clustering). However, account profile analysis is hardly applicable for detecting compromised accounts, because their profiles are the original common users' information which is likely to remain intact by spammers.

DISADVANTAGES OF EXISTING SYSTEM:

Malicious parties exploit the well-established connections and trust relationships between the legitimate account owners and their friends, and efficiently distribute spam ads, phishing links, or malware, while avoiding being blocked by the service providers.

Major OSNs today employ IP geolocation logging to battle against account compromisation. However, this approach is known to suffer from low detection granularity and high false positive rate.

URL blacklisting has the challenge of timely maintenance and update, and message clustering introduces significant overhead when subjected to a large number of real-time messages.

IV.PROPOSED WORK

Instead of analyzing user profile contents or message contents, we seek to uncover the behavioral anomaly of compromised accounts by using their legitimate owners' history social activity patterns, which can be observed in a lightweight manner.

To better serve users' various social communication needs, OSNs provide a great variety of online features for their users to engage in, such as building connections, sending messages, uploading photos, browsing friends' latest updates, etc. However, how a user involves in each activity is completely driven by personal interests and social habits. As a result, the interaction patterns with a number of OSN activities tend to be divergent across a large set of users. While a user tends to conform to its social patterns, a hacker of the user account who knows little about the user's behavior habit is likely to diverge from the patterns.

In sight of the above intuition and reasoning, we first conduct a study on online user social behaviors by collecting and analyzing user click streams of a well known OSN website. Based on our observation of user interaction with different OSN services, we propose several new behavioral features that can effectively quantify user differences in online social activities. For each behavioral feature, we deduce a behavioral metric by obtaining a statistical distribution of the value ranges, observed from each user's click streams. Moreover, we combine the respective behavioral metrics of each user into a social behavioral profile, which represents a user's social behavior patterns.

ARCHITECTURE

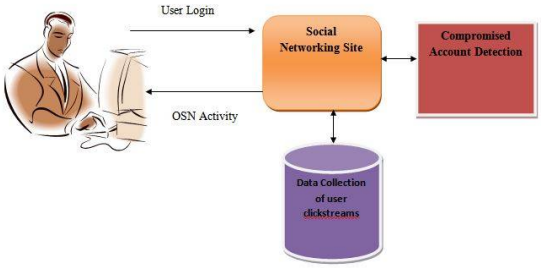

Fig 1 System Architecture.

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

IMPLEMENTATION

OSN System Construction Module

In the first module, we develop the Online Social Networking (OSN) system module. We build up the system with the feature of Online Social Networking. Where, this module is used for new user registrations and after registrations the users can login with their authentication.
Where after the existing users can send messages to privately and publicly, options are built. Users can also share post with others. The user can able to search the other user profiles and public posts. In this module users can also accept and send friend requests.
With all the basic feature of Online Social Networking System modules is build up in the initial module, to prove and evaluate our system features.

Building Social Behavior Features:

In this module, we develop the system by building social behavior features module. We categorize user social behaviors on an OSN into two classes, extroversive behaviors and introversive behaviors.
Extroversive behaviors, such as uploading photos and sending messages, result in visible imprints to one or more peer users; introversive behaviors, such as browsing other users' profiles and searching in message inbox, however, do not produce observable effects to other users. Extroversive Behaviors directly reflect how a user interacts with its friends online, and thus they are important for characterizing a user's social behaviors.
Although invisible to peer users, introversive behaviors make up the majority of a user's OSN activity; as studied in previous work the dominant (i.e., over 90%) user behavior on an OSN is browsing. Through introversive activities users gather and consume social information, which helps them to form ideas and opinions, and eventually, establish social connections and initiate future social communications. Hence, introversive behavior patterns make up an essential part of a user's online social behavioral characteristics.

Data Collection of User Clickstreams:

In this module we develop the data collection process using the Click Streams. The clickstreams in our dataset are organized in units of "sessions". We denote the start of a session when a user starts to visit our OSN in any window or tab of a browser; the end of a session is denoted when the user closes all windows or tabs that visit our OSN, or navigates away from our OSN in all windows or tabs of the browser. Clickstreams from concurrently opened tabs/windows are grouped into a single session, but are recorded individually (i.e., events from one window/tab are not merged with those from another window/tab).
We further process each clickstream before performing detailed measurement analysis. We detect and remove clickstreams in the "idle" periods—significantly long time intervals in which no user activity is observed, by analyzing the request timestamp and URLs. For example, users may go away from their computers while leaving their browsers running. With idle periods removed, we plot the "effective" cumulative clickstream lengths for each participating user.
We observe that the clickstream lengths follow exponential distribution. During a three-week period, the least active user only accumulates half an hour of activities. We also plot the Cumulative Distribution Function (CDF) of single session lengths across all users. It is evident that the distribution of single session length is heavy-tailed.

Compromised Account Detection:

In this module, we first detail the formation of a user social behavioral profile using our proposed behavioral features.
Based on our OSN measurement study, we quantify OSN user behavior patterns into a set of three metrics that correspond to the social behavioral features.
The social behavior profile of an individual user can thus be built by combining the respective social behavioral

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

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

metrics. Then, we describe the application of social behavior profiles in differentiating users and detecting compromised accounts.

The social behavioral profile depicts various aspects of a user's online social behavior patterns, and it enables us to quantitatively describe the differences in distinct user social behaviors. In this module, we first describe how to compare social behavioral profiles by calculating their difference. Then, we discuss the application of social behavioral profile comparison to distinguishing different users and detecting compromised accounts. Together with the self variance, we can apply profile comparison to distinguish different users and detect compromised accounts.

V. CONCLUSION

In this paper, we propose to build a social behavior profile for individual OSN users to characterize their behavioral patterns. Our approach takes into account both extroversive and introversive behaviors. Based on the characterized social behavioral profiles, we are able to distinguish a users from others, which can be easily employed for compromised account detection. A user's statistical distributions of those feature values comprise its behavioral profile. While users' behavior profiles diverge, individual user's activities are highly likely to conform to its behavioral profile. Our evaluation on sample Facebook users indicates that we can achieve high detection accuracy when behavioral profiles are built in a complete and accurate fashion.

REFERENCES

[1] 250,000 Twitter Accounts Hacked. [Online]. Available:http://www.cnn.com/2013/02/01/tech/social-media/twitter-hacked, accessed Sep. 2013.
[2] 50,000 Facebook Accounts Hacked. [Online]. Available:http://www.ktsm.com/news/thousands-of-facebook-accounts-hacked,accessed Sep. 2013.
[3] Detecting Suspicious Account Activity. [Online]. Available:http://googleonlinesecurity.blogspot.com/2010/03/detecting-suspiciousaccount-activity.html, accessed Sep. 2013.
[4] Facebook Tracks the Location of Logins for Better Security. [Online].Available: http://www.zdnet.com/blog/weblife/facebook-adds-bettersecurity-tracks-the-location-of-your-logins/2010, accessed Sep. 2013.
[5] Y. Bachrach, M. Kosinski, T. Graepel, P. Kohli, and D. Stillwell, "Personality and patterns of Facebook usage," in Proc. 3rd Annu. ACM Web Sci. Conf. (WebSci), Evanston, IL, USA, 2012, pp. 24–32.
[6] F. Benevenuto, T. Rodrigues, M. Cha, and V. Almeida, "Characterizing user behavior in online social networks," in Proc. 9th ACM SIGCOMM Conf. Internet Meas. Conf. (IMC), Chicago, IL, USA, 2009, pp. 49–62.
[7] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, "Aiding the detection of fake accounts in large scale social online services," in Proc. 9th USENIX Conf. Netw. Syst. Design Implement. (NSDI), San Jose, CA, USA, 2012, p. 15.
[8] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "COMPA: Detecting compromised accounts on social networks," in Proc. Symp. Netw. Distrib. Syst. Secur. (NDSS), San Diego, CA, USA, 2013..