Enhancing compromised account detection in online social networking

[1]Darshana Chaudhari, [2]sayali revade, [3]Yogita sonje, [4]Yogita Jagtap, [5]Jyoti Deshmukh
[1]UG Student, [2]UG Student, [3]UG Student, [4]UG Student, [5]UG Student Guide
[1]computer enggineering,
[1]JSPM,S BSIOTR, pune, India

***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.**

***Index Terms*— OSNs, user behavior, data analysis, compromised accounts detection**

- **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.

Related Work

[1] Proposed System detects Towards Detecting Compromised Accounts on Social Networks. Proposed methods assist in to detect and prevent three real-world attacks against popular companies and news agencies.

Limitation: Attacker who has knowledge of COMPA can prevent account from detection. Automated crawling slowing down such data gathering endeavors. COMPA can be easily extended with additional and more Comprehensive similarity measures.
Future scope: Other similarity measures integration is scope of work.

[2] This article presents investigative work on how users' activity on Face book relates to their personality, as measured by the standard Five Factor Model. Results show significant relationships between personality traits and various features of Face book profiles. We then show how multivariate regression allows prediction of the personality traits of an individual user given their Facebook profile.
Limitations: Data used may suffer from a self-selection bias. users were able to control the information stored regarding their profile, so we only had data for users who chose to let us access this information.
Future scope: Online advertising and recommender systems

[3] Website portal focuses on social networking accounts that have been hacked and estimates that 50000 password and use rid been stolen.
Limitations: Privacy and security on social network is at stake.
Future scope: Better privacy and security in social networks.

[4] Present new kind analysis of user workloads in online social networks. Our study is based on detailed click stream 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. Analysis demonstrates power of using click stream data in identifying patterns in social network workloads and social interactions. Browsing, which cannot be inferred from crawling publicly available data, accounts for 92% of user activities.
Limitation: Huge data is been crawled and hence need better algorithms for optimized processing.
Future Scope: Future analysis work is finding Impact of friends on behavior of user of social networks. Interested in understanding content distribution patterns across multiple OSNs. social Network workload generator and Markov models.

- **System Overview**

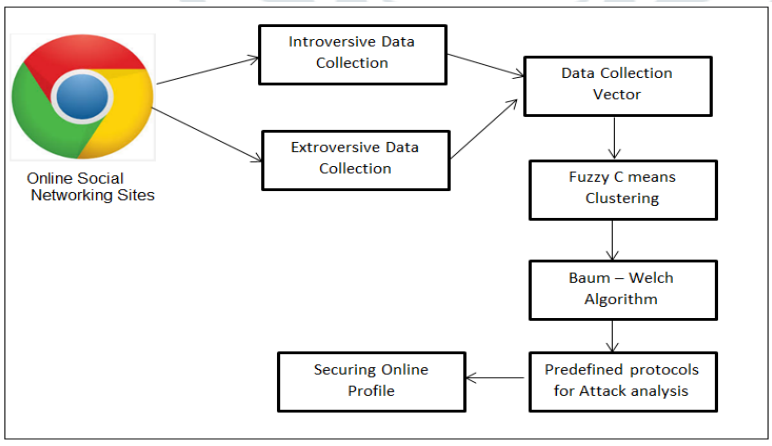

Figure 1. System overview

Social Behavior Features:

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. While most previous research only focus on the extroversive behaviors, such as public posting [8], we study both classes of behaviors for a more complete understanding and characterization of user social behaviors.

A. Extroversive Behavior Features:

Extroversive Behaviors directly reflect how a user interacts with its friends online, and thus they are important for characterizing a user's social behaviors.

B. Introversive Behavior Features:

Although invisible to peer users, introversive behaviors make up the majority of a user's OSN activity; as studied in previous work [6], [15] 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. We propose the following four features to portray a user's introversive behavior.

1.Fuzzy C- Means Clustering :

Here in this step all the data collected in above two steps are been formatted and collected in a list. And then this list is been subjected to labeling of the entities for numerical conversions and then based on this data is been converted into clusters of the desires facts by using Fuzzy C means process.
Here all the data that is been collected for the calming of insurance is clustered logically using c means clustering with the following technique. This algorithm works by assigning membership to each data point corresponding to each cluster center on the basis of distance between the cluster center and the data point. More the data is near to the cluster center more is its membership towards the particular cluster center. Clearly, summation of membership of each data point should be equal to one. After each iteration membership and cluster centers are updated according to the formula.

2.Baum_ Welch Methodology :

The Baum Welch algorithm is used to extract the hidden states from the k known parameters like introversive and extroversive entities and Baum Welch algorithm is mentioned below.

Baum- Welch Algorithm
// Input : Data Set D,
Observed States Os = { Os1 , Os2,Os3}
Step 0: Start
Step 1: Identify the Observed state Attribute Osi
Step 2: FOR i=0 to size of D
Step 3: Identify Attribute Osi and put in separateList OSL
Step 4: END FOR
Step 5: Transaction count Tc=0
Step 6: FOR i=0 to size of OSL
Step 7: identify a and ß
Step 8: Compute using Equation1
Step 9:IF belongs to Os

Step 10: THEN add Hs (Hidden State) to list
Step 11: END FOR
Step 12: Stop

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. 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.Proper identification of hidden states of attack.

References

[1]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.
[2]F. Schneider, A. Feldmann, B. Krishnamurthy, and W.Willinger, "Understanding online social network usage from a network perspective,"Proc. 9th ACM SIGCOMM Conf. Internet Meas. Conf. (IMC), Chicago,IL, USA, 2009, pp. 35–48.
[3]G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks,"in Proc. 26th Annu. Comput.Secur. Appl. Conf. (ACSAC),Austin, TX, USA, 2010, pp. 1–9.
[4]FabrícioBenevenutoy Tiago RodriguesyMeeyoungChalVirgílio 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.
[5] Tiago Rodrigues Meeyoung Cha Virgílio Almeida "Characterizing User Behaviorin Online Social Networks" in proc13
[6] Y. Xie*et al.*, "Innocent by association: Early recognition of legitimate users," in *Proc. ACM Conf. Comput. Commun.Secur.(CCS)*, Raleigh, NC, USA, 2012, pp. 353–364
[7] H. Xiong, P. Malhotra, D. Stefan, C. Wu, and D. Yao, "User-assisted host-based detection of outbound malware traffic," in *Proc. 11th Int.Conf. Inf. Commun. Secur. (ICICS)*, Beijing, China, 2009, pp. 293–307.
[8] C. Yang, R. Harkreader, J. Zhang, S. Shin, and G. Gu, "Analyzing spammers' social networks for fun and profit: A case study of cyber criminal ecosystem on Twitter," in *Proc. 21st Int. Conf. World WideWeb (WWW)*, Lyon, France, 2012, pp. 71–80.

[9] C. Yang, R. C. Harkreader, and G. Gu, "Die free or live hard? Empirical evaluation and new design for fighting evolving Twitter spammers," in *Proc. 14th Int. Conf. Recent Adv. Intrusion Detection (RAID)*, Menlo Park, CA, 2011, pp. 318–337.