In Social Networking Sites Solutions for The Frauds And Threats

Shadab Adam Pattekari[1], Dr. Ravindra Nath Katiyar[2]
[1, 2] Dept of Computer Science and Engineering
[1, 2] University Institute of Engineering & Technology, CSJMU, Kanpur

Abstract- *Internet with Social media have open the new ways of communication in the hyper connected world. This communication involves tweets, sharing photos, images, likes and comments etc. among the people all around the world. Many users join multiple social networks for different purposes and enter personal and other specific information covering social, professional. The problem of fraud detection is concern with not only capturing the fraudulent activities, but also capturing them as quickly as possible. Now a days there are many terror attacks happened by using social network, such a terrorist attacks are hazardous for peoples, organizations and countries. Terrorist are using internet to spread terror and form terrorist group. Integration of multiple online and real social networks makes the users vulnerable to unintentional and intentional security threats and misuse. Data mining techniques provide researchers and practitioners the tools needed to analyze large, complex, and frequently changing social media data. We present an overview of existing solutions that can provide better protection, security, and privacy for online social network users.*

Keywords- social networks, security and privacy, data mining, threat modeling.

I. INTRODUCTION

Social networking sites are an online platform that people use to build social networks or social relations with other people. They can share similar personal or career interests, activities, backgrounds or real-life connections. Social networking services are Internet-based applications.

IN recent years, global online social network (OSN) usage has increased sharply. OSNs, such as Facebook , Google+ , LinkedIn ,Twitter, and have hundreds of millions of daily active users. Unfortunately, many OSN users are unaware of the security risks which exist in these types of communications, including privacy risks, identity theft, malware, fake profiles and sexual harassment among others.

Social Media sites can also be referred to as web-based services that allow individuals to create a public/semi-public profile within a domain such that they can communicatively connect with a list of other users within the network. Social Media is an important source of learning of opinions, sentiments, subjectivity, assessments, approaches, evaluation, influences, observations, feelings, borne out in text, reviews, blogs, discussions, news, remarks, reactions, or some other documents.

II. LITERATURE REVIEW

Text data on the web is the best content type on the net when it comes to author's opinion. Recently, following the progress of wireless internet and smartphone devices, iPhones the amount of data on the web is increasing with no limit to time or location. This method of learning Typical–Terrorist-Behavior is represents the typical behavior of terrorist users based on the content of their web activities. It is believed that it is possible to collect web pages from terror-related sites, and it is possible to use them for their inhuman actions. The content of the collected pages is the input to the Vector Generator module that converts the pages in to the vectors. These vectors are stored in the use of future processing in the vector of terrorists transactions data base. The web pages are clustered by using unsupervised of clustering technique [2]. Clusters serve as data indicating the typical terrorist behavior or the profile of the terrorist or their supporters.

One major issue of today is the representation of textual content of Web pages. Specifically, there is a necessity to represent the data of terror-related pages as against the content of a currently accessed page in order to compute the similarity between them.

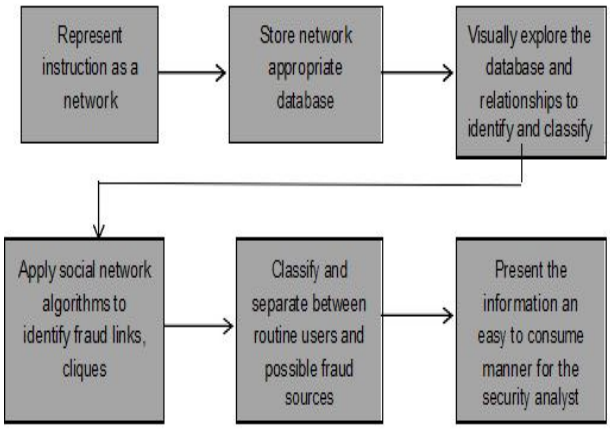
III. SOCIAL NETWORK ANALYSIS:

Social Network Analysis (SNA) is one of the most used technologies for studying criminal and terrorist networks. It is the one of the data mining methods in fraud analytics, is a technique which represents the entities as nodes and the relationships between the entities as links. The SNA technique represents the role between the actors within the social networks. In the fraud detection, the interaction and exchanges can be viewed as heterogeneous networks with multiple participants. The numbers of participants are generally huge, but the kind of interaction among the individuals is generally

in limits only and known. Graph analysis techniques can used further to identify suspicious individuals, groups, relationships, unusual changes over time/geography, and anomalous networks within the overall graph structure.

.

Figure 1: End to end fraud analytics approach using social network analysis methods



IV.THREATS

With the increasing usage of OSNs, many users have un-knowingly become exposed to threats both to their privacy and security. These threats can be divided into four main categories. The first category contains classic threats namely, privacy and security threats. The second category covers modern threats that use the OSN infrastructure to endanger user privacy and security. The third category consists of combination threats, where we describe how today's attackers can, and combine various types of attacks. The fourth and last category includes threats specifically targeting children who use social networks.

Following are top 10 Social Networking Threats.

1. Social networking worms: Social networking worms include Koobface, which has become, according to researchers, "the largest Web 2.0 botnet." While a multi-faceted threat like Koobface challenges the definition of "worm," it is specifically designed to propagate across social networks, enlist more machines into its botnet, and hijack more accounts to send more spam to enlist more machines. All the while making money with Social Network Analysis is having an ability to detect subgroups and discovering their patterns of the interaction, and identifying central individuals the usual botnet business, including scareware and Russian dating services.

2. Phishing bait: Many Facebook users had their accounts compromised, and although it was only a "tiny fraction of a percent," when you realize Facebook has over 350 million users, it's still a significant number. To its credit, Facebook acted quickly, working to blacklist that domain, but lots of copycat efforts ensued (e.g., fbstarter.com). Facebook has since gotten rather adept at Whack-A-Mole.

3. Trojans: Social networks have become a great vector for trojans -- "click here" and you get:
* Zeus -- a potent and popular banking Trojan that has been given new life by social networks.
* URL Zone -- is a similar banking Trojan, but even smarter, it can calculate the value of the victim's accounts to help decide the priority for the thief.

4. Data leaks: Social networks are all about sharing. Unfortunately, many users share a bit too much about the organization -- projects, products, financials, organizational changes, scandals, or other sensitive information. Even spouses sometimes over-share how much their significant other is working late on top-secret project, and a few too many of the details associated with said project. The resulting issues include the embarrassing, the damaging and the legal.

5. Shortened links: People use URL shortening services to fit long URLs into tight spaces. They also do a nice job of obfuscating the link so it isn't immediately apparent to victims that they're clicking on a malware install, not a CNN video. These shortened links are easy to use and ubiquitous. Many of the Twitter clients will automatically shorten any link. And folks are used to seeing them.

6. Botnets: Late last year, security researchers uncovered Twitter accounts being used as a command and control channel for a few botnets. The standard command and control channel is IRC, but some have used other applications -- P2P file sharing in the case of Storm -- and now, cleverly, Twitter. Twitter is shutting these accounts down, but given the ease of access of infected machines to Twitter.

7. Advanced persistent threats: One of the key elements of advanced persistent threats (APT) is the gathering of intelligence of persons of interest for which social networks can be a treasure trove of data. Perpetrators of APTs use this information to further their threats -- placing more intelligence gathering (e.g., malware, trojans), and then gaining access to sensitive systems. So while not directly related to APTs, social networks are a data source.

8. Cross-Site Request Forgery (CSRF): While it isn't a specific kind of threat -- more like a technique used to spread a sophisticated social networking worm, CSRF attacks exploit the trust a social networking application has in a logged-in

user's browser. So as long as the social network application isn't checking the referrer header, it's easy for an attack to "share" an image in a user's event stream that other users might click on to catch/spread the attack.

9. Impersonation: The social network accounts of several prominent individuals with thousands of followers have been hacked. Furthermore, several impersonators have gathered hundreds and thousands of followers on Twitter and then embarrassed the folks they impersonate. Twitter will now shut down impersonators attempting to smear their victims, but at Twitter's discretion. Admittedly, most of the impersonators aren't distributing malware, but some of the hacked accounts certainly have.

10. Trust: The common thread across almost all of these threats is the tremendous amount of trust users have in these social applications. Like e-mail, when it hit the mainstream, or instant messaging when it became ubiquitous, people trust links, pictures, videos and executables when they come from "friends," until they get burned a few times. Social applications haven't burned enough people yet. The difference with social networks is that the entire purpose of them is to share a lot which will result in a steeper learning curve for users.

Solution to Threats

In recent years, social network operators, security companies, and academic researchers have tried to deal with the above-mentioned threats by proposing a variety of solutions. In this section we describe possible solutions which can assist in protecting the security and privacy of OSN users.

A. Social Network Operator Solutions

OSN operators attempt to protect their users by activating safety measures, such as employing user authentication mechanisms and applying user privacy settings. Several of these techniques are described in detail below.

Authentication Mechanisms:

In order to make sure the user registering or logging into the social network is a real person and not a social bot or a compromised user account, OSN operators use authentication mechanisms, such as CAPTCHA, photos-of-friends identification , multi-factor authentication, and in some cases even requesting that the user send a copy of his or her government issued ID. As an example, Twitter recently introduced its two-factor authentication mechanism, requiring the user to not only insert a password when logging into Twitter but also provide a verification code that was sent to the user's mobile device. This mechanism prevents a malicious user from logging in through hijacked accounts and publishing false information through those hijacked accounts. Such a mechanism would the wart incidents such as when hackers hijacked the Associated Press (AP) Twitter account, resulting in the rapid propagation of false information about explosions in the White House, which caused panic on Wall Street.

Security and Privacy Settings:

Many OSNs support various configurable user privacy settings that enable users to protect their personal data from other users or applications. Facebook users, for example, can customize their privacy settings and choose which other users in the network are able to view their details, pictures, posts, and other personal information. Some OSNs also support extra security configurations which enable the user to activate secure browsing, receive login notifications, and establish other safety features. However, many OSN users still simply maintain the default privacy settings, letting their data be exposed to strangers.

Internal Protection Mechanisms:

Several OSNs protect their users by implementing additional internal protection mechanisms for defense against spammers, fake profiles, scams, and other threats. Facebook, for example, protects its users from malicious attacks and information collecting by activating the Facebook Immune System (FIS). The FIS is described as an adversarial learning system that performs real-time checks and classifications on read-and-write actions on Facebook's database.

Report Users:

OSN operators can attempt to protect young children and teenage users from harassment by adding an option to report abuse or policy violations by other users in the network. In some countries, social networks like Facebook and Bebo have also added a "Panic Button" to better protect children.

B. Commercial Solutions

Various commercial companies have expanded their traditional Internet security options and now offer software solutions specifically for OSN users to better protect themselves against threats. In this section, we present mainstream software and application-protection solutions which were developed by well-known security companies, such as Symantec and Check Point, as well as solutions which

were created by several startup companies, such as Online Permissions Technologies, and open-source solutions, such as No Script Security Suite.

Internet Security Solutions:

Many security companies, like AVG, Avira, Kaspersky, Panda, McAfee, and Symantec, offer OSN users Internet security solutions. These software suites typically include anti-virus, firewall, and other. Internet protection layers which assist OSN users in shielding their computers against threats such as malware, click jacking, and phishing attacks. For example, McAfee Internet Security software provides its users with protection against various threats such as malware, botnets, and inappropriate sites AVG Privacy Fix : AVG Privacy Fix is software available as a mobile application or a web browser add-on which offers its users a simple way to manage their privacy settings on Facebook, LinkedIn, and Google. Additionally, Privacy Fix helps its users block over 1200 trackers by following their movements online. The software also tells its users how much revenue they are generating for Facebook and Google.

FB Phishing Protector:

FB Phishing Protector is a Firefox add-on which warns Facebook users when a suspicious activity is detected, such as a script-injection attempt. This add-on provides protection against various phishing attacks.

Norton Safe Web:

Symantec's Norton Safe Web is a Facebook application with more than 500 000 users. It scans the Facebook user's News Feed and warns the user about unsafe links and sites.

McAfee Social Protection:

McAfee Social Protection is a mobile application which enables Facebook users to safe-guard their uploaded photos by letting users control precisely who can view and download their images.

My Permissions:

Online Permissions Technologies' My Permissions is a web service that provides its users with convenient links to the permissions pages for many OSNs, such as Facebook, Twitter, and LinkedIn. These links can help users view and revoke the permissions they had given in the past to various applications, thus better protecting their privacy. Additionally, My Permissions offers periodic email reminders that prompt users to check their OSN permissions settings.

No Script Security Suite:

No Script Security Suite is an open-source extension to Mozilla-based web browsers like Firefox, which allows executable web content such as JavaScript, Java, and Flash to run only from trusted domains of the user's choice. Blocking executable web content running from untrusted sites can protect OSN users from click jacking and XSS attacks.

Privacy Scanner for Facebook:

Trend Micro's Privacy Scanner for Facebook is an Android application which scans the user's privacy settings and identifies risky settings which may lead to privacy concerns. It then assists the user in fixing the settings.

Defensio:

Websense's Defensio web service helps protect social network users from threats like links to malware that could be posted on the user's Facebook page. The Defensio service also assists in preventing information leakage by controlling the user's published content by removing certain words from posts or filtering specific comments.

Zone Alarm Privacy Scan:

Check Point's Zone Alarm Privacy Scan is a Facebook application which scans recent activity in the user's Facebook account to identify privacy concerns and to control what others can see. For instance, Zone Alarm Privacy Scan can identify posts that expose the user's private information.

Net Nanny:

Content Watch's Net Nanny is software which assists parents in protecting their children from harmful content. Net Nanny lets parents monitor their children's social media activity on different OSN websites, such as Facebook, Twitter, and Flickr.

Minor Monitor:

In foglide's Minor Monitor is a parental control web service which gives parents a quick dashboard view of their child's Facebook activities and online friends. By using Minor Monitor, parents can be informed about questionable content that may have been revealed to their child, and they can identify over-age friends in their child's Facebook friends list.

C. Academic Solutions

Several recently published studies have proposed solutions to various OSN threats. These solutions have primarily focused on identifying malicious users and applications. In this sec- tion, we present studies which provide solutions for improving OSN users' privacy settings; for detecting phishing, spammers, cloned and fake profiles, and socware; and for preventing information and location leakage.

These academic solutions provide cutting-edge insight into dealing with social network threats. They can be used by OSN operators to improve their users' security and privacy, by security companies to offer the customers better OSN protection, or by early-adopter OSN users who want to better protect themselves.

Phishing Detection:

Many researchers have suggested anti-phishing methods to identify and prevent phishing attacks; most of these methods have been based on techniques that attempt to identify phishing websites and phishing URLs.With the increasing number of phishing attacks on OSNs, several researchers have suggested dedicated solutions for identifying social network phishing attacks. Introduced Warning Bird, a suspicious URL detection system for Twitter which can handle phishing attacks that conceal themselves by using conditional redirection URLs. Later in the same year, Aggarwal presented the Phish Ari technique, which can detect whether or not a tweet posted with a URL is phishing by utilizing specific Twitter features such as the account age and the number of followers of the user who posted the suspicious tweet.

Spammer Detection:

Many researchers have recently proposed solutions for spammer detection in OSNs. In 2009,Benevenut offered algorithms for detecting video spammers which succeeded in identifying spammers among YouTube users. In 2010, DeBarr and Wechsler used the graph centrality measure to predict if a user is likely to send spam messages. Wang proposed a method to classify spammers on Twitter by using content and social network graph properties. Stringhini created more than 300 fake profiles (also referred to as "honey-profiles") on Twitter, Face-book, and MySpace and successfully identified spammers who sent spam messages to the fake profiles. Lee also presented a method for detecting social spammers of different types by using honeypots combined with machine learning algorithms. In 2013, Aggarwal presented machine learning algorithms for detecting various type of spammers in Foursquare. Recently, Bhat and Abulaish introduced a community-based framework to identify OSN spammers. Also,Verma presented a survey which reviews existing techniques for detecting spam users on Twitter.

Cloned Profile Detection:

In 2011, Kontaxis proposed a methodology for detecting social network profile cloning. They designed and implemented a prototype which can be employed to investigate whether or not users have fallen victim to clone attacks. In 2013, Shan presented the Clone Spotter which can be deployed into the OSN infrastructure and can detect cloning attacks by using users' data records,such as a user's login IP records that are available to the OSN operator.

Fake Profile Detection:

In recent years, researchers have developed algorithms, techniques, and tools to identify fake profiles and prevent various sybil attacks via OSNs. In 2006,Yu presented the Sybil Guard decentralized protocol that assists in preventing sybil attacks. Later, in 2008, Yu also presented the Sybil Limit protocol, a near-optimal defense against sybil attacks using social networks. In 2009, Danezis and Mittal offered the Sybil Infer defense algorithm which can distinguish between "honest" and "dishonest" users. In the same year, Tran presented the Sum Up sybil defense system to limit the number of fake votes cast by sybils. In 2012, Cao introduced the Sybil Rank tool which utilizes OSN graph properties to rank users.

Although the common goal of both fake profile algorithms and sybil defense algorithms is to identify fake profiles, a difference exists: Fake profile detection algorithms seek to identify fake profiles in general, including cases of cyber predators which hold only a few fake profiles in the OSN; sybil defense algorithms are a private case of fake profile detection algorithms and are usually intended to identify attackers who create a large number of fake profiles in the OSN. Later, they deployed Sybil-Rank in the operation center of Tuenti, the largest OSN in Spain, and estimated that about 90% of the 200 000 users who received the lowest rank were actually fake profiles. In the same year, Wang proposed a crowd sourced fake profiles detection system and evaluated it using data from Facebook and from a Chinese OSN. Also, in 2012, Fire presented an algorithm for identifying malicious profiles using the social network's own topological features. They evaluated their methods on three directed OSNs—Academia.edu, Any beat and Google+—and succeeded in identifying fake profiles and spammers. Fire also presented

The Social Privacy Protector application which assists Face-book users in identifying fake profiles among their friends.
They used the dataset created by The Social Privacy Protector application and developed machine learning classifiers which can identify fake profiles on Facebook. Recently, Wang
presented a system which can detect fake profiles based on analyzing clickstream models. Additional surveys regarding solutions to sybil attacks have also been presented by Levine and by Hoffman.

Socware Detection:

In the last few years, several studies have tried to better understand and identify socware. In 2012,Rahman presented the My Page Keeper Facebook application that aims to protect Facebook users from damaging posts on their timelines. Rahman also presented Facebook's Rigorous Application Evaluator (FRAppE) for detecting malicious applications on Facebook. In 2013,Huang studied the socware ecosystem and discovered several insights about socware propagation characteristics that can assist in future research on the detection and prevention
of socware propagation.

Preventing Information and Location Leakage:

In their study on privacy leaks on Twitter, Mao offered a"guardian angel service" that can monitor users' tweets and alert users to potential privacy violations. Their offered solution can be based on classifiers they constructed throughout their study which can identify tweets containing private information,such as vacation plans. Moreover, Gómez-Hidalgo used Named Entity Recognition (NER) algorithms to prevent data leakage. In their study, they implemented a prototype to demonstrate how their methods can prevent data leakage. Their methods may also be used to prevent OSN users from exposing their locations. Recently, Ghiglieri presented the

Personal DLP tool to help OSN users better understand and evaluate the sensitivity of their posted statuses. The study included 221 participants, and the developed Personal DLP prototype was found to have a positive impact on users' privacy awareness.

V. CONCLUSION

In this paper we study about what is the data mining, and explores the major developments to detect the terrorist networks. The purpose of this detection process is to powerfully detect and stop the terrorist activities. In present paper SNA introduces the detection process through network analysis in the form of a graph and cluster analysis for subgroup detection. The Intrusion detection system (IDS) monitors all the activities of terrorist and terrorist organization. After that the learning Typical Terrorist behavior model which monitors all the terrorist behavior by using unsupervised clustering technique. This case study consider the most relevant problems in social network analysis from fraud detection point of view and to restrict the terrorist activities.

By using this new techniques we can stop terrorism and to stop terrorist to fulfill their inhuman goals.

REFERENCES

[1] Sequeira, K., Zaki, M. (2002) ADMIT: Anomaly-based Data Mining for Intrusions, Proceedings of SIGKDD 02, pp. 386-395, ACM.
[2] Mohammad Javad Hosseinpour, Mohammad Nabi Omidvar, "Detecting Terror-Related Activities on the Web with Using Data Mining Techniques", 2009 Second International
[3] Jain, A.K., Murty, M.N., Flynn, P.J. (1999) Data Clustering: A Review, ACM Computing Surveys, 31, 3:264-323.
[4] Debar, H., Dacier, H., Dacier, M., Wespi, A. (1999) Towards a taxonomy of intrusion-detection systems, Computer Networks, 31, pp. 805–822.
[5] Kelley, J. (2002) Terror Groups behind Web, encryption, USA Today, URL:http://www.apfn.org/apfn/WTC_why.htm
[6] Hosseinpour, M.J.; Omidvar, M.N., (2009) "Detecting Terror Related Activities on the Web with Using Data Mining Techniques", Proceedings of the Second International Conference on Computer and Electrical Engineering, 2009(ICCEE '09), Vol 2, 152-157.
[7] German Florez, Susan M. Bridges, and Rayford B. Vaughn (2002) "An Improved Algorithm for Fuzzy Data Mining for Intrusion Detection", Proceedings of NAFIS2002 Annual Meeting of the North America, 457-462.
[8] Shingo Mabu, Member, Ci Chen, Nannan Lu, Kaoru Shimada, and Kotaro Hirasawa,(2011) "An Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming", Proceedings of the IEEE Transactions on Systems, Man, and Cybernetics—Part c: Applications and Reviews, Vol. 41, No. 1, 132-139.