Review of Security Approaches for Social Networking

Bhagyashree Patil
Department of Computer Engineering
MIT College of Engineering
Pune, India

Sambhaji Sarode
Department of Computer Engineering
MIT College of Engineering
Pune, India

Abstract— **Social networking uses different applications and dedicated websites for the communication to the user located at remote site. People having similar interest are connected through social networking. Online social networking uses different websites. Such websites are called as social networking sites. Social networking creates community of interested users. Online communities shares hobbies, common interest, lifestyle, views, politics, and knowledge. Sharing will helps even reading the profiles of other users, commenting on status, contacting others users indirectly. Ultimately personal information of any user can be known by any other easily. Misuse of personal information disturbs the mental, physical, social, psychological state of mind of user. Economical loss is major impact .Rapid growth in social networking are responsible for giving rise to many attacks that are entering from cyber world to real life. Structural anomaly and psychological profiling helps to identify behavior of attacker. Using Psycho-linguistic cues deception is identified. Protection motivation theory helps to motivate online social networking user for safe surfing. Proposed incident handing framework helps learners to feel confident while online and alerts adults to manage secure online environment. All above approaches will helps social networking users to be secure in online environment.**

Index Terms— Privacy preserving, mobile social networks, cyber threats, cyber security, cyber bullying, social networking, framework, cyber safety.

I. INTRODUCTION

Popularity of social networking is increasing in schools, colleges, workplaces and organizations. Millions of users are connected to internet through social networking to gather and share first-hand information and experiences about gardening, golfing and cooking also used for developing friendships, finding employment, professional alliances, and business-to-business marketing and even groups sharing information. The interests are as varied and rich as the story of our universe.

Different networking sites usually consist of user's personal information such as date of birth, address, and phone number. Some sites also allow users to provide more information about themselves such as interests, relationship status, hobbies, favorite books, movies, and music, food.

Some social network sites are like Match.com, where most people prefer to be anonymous. Some individuals can sometimes be identified with face re-identification. In survey of two major social networking sites it is found that 15% of the similar profile pictures, photographs with similar pictures over multiple sites can be matched to identify the users.

Dangers associated with social networking including data viruses and data theft, which are rising tremendously. The most danger involves online predators or individuals who claim to be someone that they are not. Disclosing of personal information makes easier to attacker to attack on mental, physical, social, economic state of individual. Different approaches and frameworks are reviewed in this paper which gives guidelines to be aware of while doing online social networking.

Different approaches are present to detect anomaly behavior in online social networking such as:

1. Threats detection using Structural Anomaly Detection (SA) and Psychological Profiling (PP)

Graph analysis, dynamic tracking, machine learning are technology used by SA. Psychological profiles are identified from behavioral patterns in PP. Threats are identified through a fusion and ranking of outcomes from SA and PP.

2. Psycho-linguistic cues based on LIWC-

To automatically extract linguistic cues from social media based text content we can use software tools such as the Linguistic Inquiry and Word Count (LIWC). Using LIWC, from text content, up to 88 output variables can be computed. Variables give information about the linguistic style, structural composition elements and the frequencies of different linguistic categories.

3. Protection Motivation theory- PMT motivates to students to be secure from cybercrimes while using social networks.

4. Proposed role players for incident handling framework.

II. RESEARCH METHODOLOGY

A. Threats detection using Structural Anomaly Detection (SA) and Psychological Profiling (PP)

It is an approach which combines Structural Anomaly Detection (SA) from social and information networks and Psychological Profiling (PP) of individuals. Graph analysis, dynamic tracking, and machine learning are technology used to detect structural anomalies in large-scale information network data. Psychological profiles are constructed from behavioral patterns. Fusion and ranking outcomes from SA and PP are used to identify online anomaly behavior.

Data set is taken from multiplayer online games. Over a period of 6 month data set is observe that contains behavior traces from over 350,000 characters. This method describes instead of investigation after the fact, capability to proactively identify malicious intent before the intent is carried out. Structural Anomaly Detection (SA) , extracts information from large-scale information network data (social networks, messages, internet visits, etc.). SA defines similarity between individuals, normal patterns, and anomalies. PP reduces SA's false prediction rate, making the threat detection more useful.

1. Graph learning for anomaly detection using psychological context (GLAD-PC)

Graph Structure Analysis discovers information networks specific characteristics and exploits them for efficient data representation and massive data reduction. Graph Embedding converts data from a graph representation to an attribute space which is very much useful for machine learning methods. Dynamic Tracking is performed in the attribute space to monitor individual evolution over time and Anomaly Detection finds unusual patterns in graph data. SA will help to detect data anomalies not threats [1].

2. Structural Anomaly Detection (SA)

Behavioral pattern of users in information networks such as whom they contact and how frequently, are dynamic, slow-varying and with abrupt changes possibly indicating abnormal events. Anomaly detection assumes that subject behavior can be captured as a multi-variant sequence of abstract, continuous and discrete attributes Learning-based approach, which uses behavior sequences with known anomalies are used to construct a probabilistic model. Model is applied to observations to decide the likelihood of a new anomaly event. A simple baseline method such as one-class support vector machine (SVM) or nearest neighbor based methods can provide a way to demonstrate early on the ability to make anomaly judgments and provide a benchmark for future performance comparisons [2].

3. Psychological Profiling (PP)

Semantic meaning for threat detection is provided by Psychological Profiling (PP). PP is helpful in reducing data volume, reducing false alarm rate and detects suspicious intent/activity based on domain knowledge of human psychology. PP mitigates the risk that a threat could look normal from the information network data alone and would then be overlooked by the SA thread. A psychological model gives us a way to focus our investigations on individuals who have the motivation and capability to carry out an attack. Realization of a threat requires planning and preparation and depends on the emotional state and personality of the perpetrator. The emotional state is captured through psychological variables such as anger and depends on personal variables that represent both cognition and personality. These personal variables help to determine how external events trigger changes in emotional state and how changes in emotional state affect the likelihood that an insider will begin or continue a threatening activity. Each of these internal model variables can be potential associated with observable indicators. Dynamic psychological model that describes temporal patterns of activities leading up to an attack, based on relevant personality, emotional, and situational variables.

In addition to tracking static behavior patterns and social network structures, sudden changes in behavior and social network configuration are founded. Sudden changes may be indicative of an imminent insider attack.

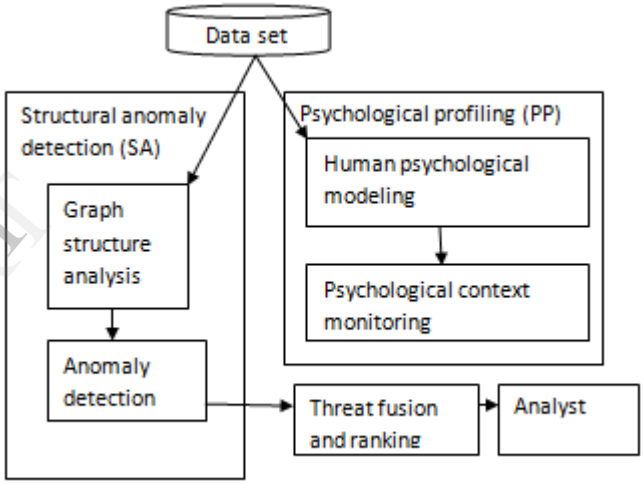

Fig.1..Threat detection using Structural Anomaly Detection and psychological profiling

4. Threat Fusion and Ranking

Bayesian method is used for Threat Fusion and Ranking, to coherently combine data about psychological anomalies and profiles, and provide threat alarms. An initial generative model can be generated from limited historical data like the Fort Hood event and a set of example scenarios covering threats and innocuous behaviors. Statistical inference method will rank threats based on their probability and uncertainty. In order to provide actionable information, severity and urgency of threats is used by ranking function.

Thus this is one of the method which tries to find out anomaly behavior of attacker before he tries to do some malicious activity.

Pros

Game data contains malicious behaviors that are identifiable. It is possible to detect anomalous behaviors

through structural analysis of social networks in the game, and to predict a player's personality from in-game behavior and feature.

Cons

Proposed approach illustrated by applying it to large data set from a massively multiplayer online game. If data set is massive then only this methodology is useful.

B. Psycho-linguistic cues based on LIWC

1. Deception

Deception is the manipulation of a message to cause a false impression or conclusion [3].

Users with hostile intent often create stories based on imagined experiences or attitudes to hide their true intent. According to psychology one's state of mind, such as physical/mental health and emotions, can be finding out by the words they use. In face-to face communication we have access to non-verbal cues such as body language, real-time adaptation of stories, etc. These cues are unavailable in Internet based communication.

2. Psycho-linguistic Modeling

It is important first to identify accurate linguistic deception indicators and model them.

Following observations have been made about some psycho-linguistic cues that indicate deception in text:

a. Fewer first-person pronouns are used as an attempt to dissociate themselves from their words.

b. Fewer exclusive words are used to keep the deceptive story simple.

c. Frequency of negative emotions words increase may be due to guilt.

d. Frequency of active verbs increase as an act of distraction.

Therefore to automatically extract linguistic cues from social media based text content we can use software tools such as the Linguistic Inquiry and Word Count (LIWC) [4]. Using LIWC for each text content 88 output variables can be computed.

Then ranking is given to these 88 variables as strong, medium and weak indicators of deception. Once the psycho-linguistic cues that are strong indicators of hostile intent are identified the next step is to statistically model and analyze or classify them.

Thus depending upon the results obtained from analysis deception is identified. Thus deception is identified by Psycho-linguistic cues based on LIWC.

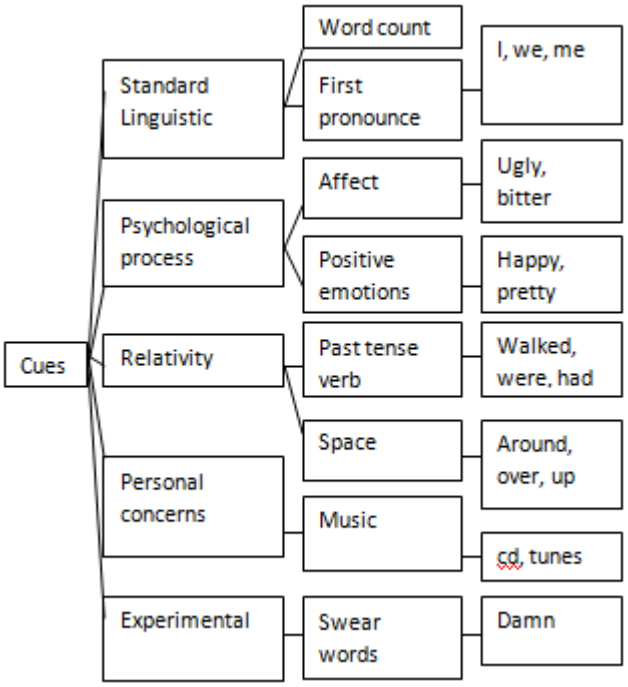

Fig.2.Psycho-linguistic Model

Pros

Psychological behavior of attacker is identified from psychological state of mind and possible attack is found out using Psycho-linguistic cues based on LIWC.

Cons

If attacker is very smart to hide it's state of mind very smartly then it is very difficult to identify the possible attacker.

C. Protection Motivation Theory

As use of social networking rapidly increasing parallel growth in cybercrime is increasing. Cyber security awareness among employees of businesses is more but less in the general population. Protection Motivation Theory making use of the five motivational factors: response cost, response efficacy, vulnerability, self-efficacy and risk severity. PMT motivates to students to be secure from cybercrimes while using social networking sites..

The sub-process of threat appraisal is comprised of a person's appraisal of the severity of the risks and the person's vulnerability to those risks. The coping appraisal sub-process is comprised of three elements: a person's assessment of their own efficacy to deal with the threat, a person's assessment of the efficacy of possible responses, and the cost of responding. These various assessments made during the cognitive process can be summarized by the questions that a person would ask themselves during the appraisal process [5].

PMT could provide a new technique for understanding use behaviors related to adoption of new technologies, particularly where perceived risk is involved.

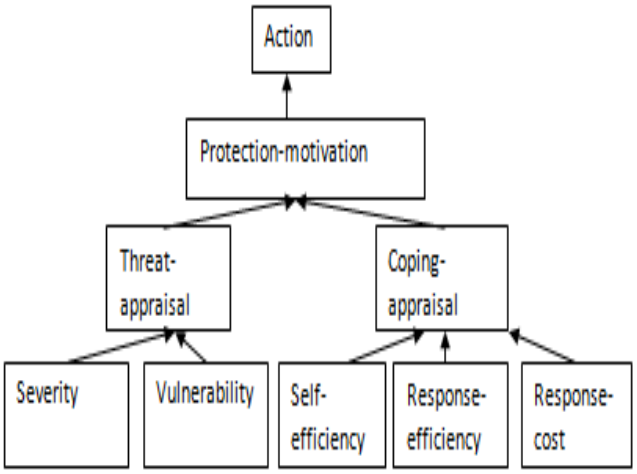

Fig.3.Protection Motivation Theory approach

Pros

A study on student motivation to act is depends upon students' observation, interviews and surveys in which PMT factors are discussed.

Cons

The younger students grow with computers they think that we know everything about computer because of that they don't try to learn more in such situation motivation act cant's help students to motivate them from cybercrime.

D. Proposed role players for the incident handling structure.

Cyber threats are direct online threats or "distressing material". There are no clear procedures that are consistently followed by governing boards, schools, educators. The cyber threat process is not widely known and understood by learners, their parents/guardians and educators. As a result, many learners remain vulnerable to the negative effects of cyber threats.

In a given structure emphasis is given on students which should be protected from cyber threats. Role players are given by taking students as center element.

1. Role players within the school.
a. Responsibilities of the principals.
b. Responsibilities of the educators.
c. Information technology unit.
d. Responsibilities of learners.

2. Role players outside the school.
a. Responsibilities of parents.
b. Responsibilities of industry.
c. Responsibilities of government.
d. Non-governmental organizations.

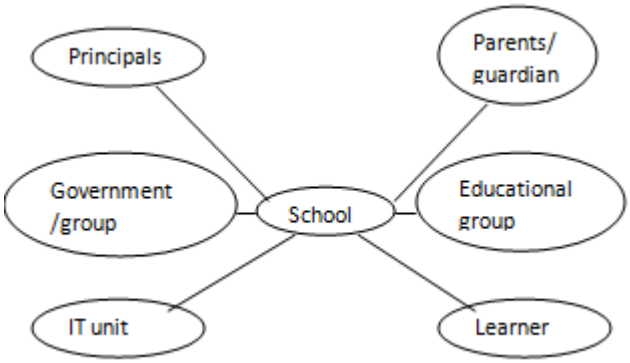

Fig.4. Proposed role players for the incident handling structure

Hence along with the learners, schools, organizations, government should also take care about the secure online activities.

Pros

Thus framework is beneficial feel confident to learners while online and alert adults manage secure online environment.

Cons

If learner, parents, guardians school management system etc. are not aware of possible attacks happens during online social networking then framework fails to create secure online environment.

Psycho-linguistic cues based on LIWC.	**Proposed incident handling framework.**	**SA and PP**	**A Study on Student Motivation to Act**
Psycho-linguistic cues based on LIWC helps to detect hostile intent in social media. It is a method to detect deception from Text data generated in the context of social media communications. Deception is the manipulation of a message to Cause a false impression or conclusion.	This paper gives proposed incident handling framework for schools in South Africa. This framework is helpful to learner to take decision what to do when they are threaten online.	This paper proposes an approach that combines Structural Anomaly Detection(SA) And psychological Profiling (PP) of users. Graph analysis, dynamic tracking and machine learning technique are used by SA. Psychological profiles are constructed from behavioral patterns by PP.	This paper focuses on the general student population at Kennesaw State University (KSU).Students from KSU are motivated to protect them from the cybercrime. Roger's Protection Motivation Theory helps student to motivate which uses five major factors.
Psychology suggests that one's state of mind, such as physical/mental health and emotions, can be identified by the words they use.	Parents, teachers, principals, learners, school management team all are role players during secure social networking.	Proposed approach illustrated by applying it to large data set from a massively multiplayer online game.	A study on student motivation to act is depends upon students' observation, interviews and surveys in which PMT factors are discussed.
Thus such Psychological behavior of attacker is identified and possible attack is find out using Psycho-linguistic cues based on LIWC.	Thus framework is beneficial feel confident to learners while online and alert adults manage secure online environment.	Game data contains malicious behaviors that are identifiable. It is possible to detect anomalous behaviors through structural analysis of social networks in the game, and to predict a Player's personality from in-game behavior and feature.	The younger students grow with computers they think that we know everything about computer because of that they don't try to learn more in such situation motivation act cant's help students to motivate them from cybercrime.

Table 1.Comparison of four approaches for cyber security

III. CONCLUSION

Social networking allows users to share different resources at any time but together with it immerges with social issues which threaten the social, physical, psychological state of the user. Also cause the economic issues because of inception in personal information of user.

Many approaches are suggested to protect from cyber threat depending on anomaly detection and psychological state of attacker. But

All these approaches have not given 100% grantee of security.

Hence it is personal responsibility of every user to do social networking securely to protect from social, physical, psychological, economical damage.

IV. ACKNOWLEDGEMENT

We would like to thanks mentors for valuable discussions, contributing the ideas and helping us to solve problems.

REFERENCES

1. Burt, R. (1995). Structural holes: the social structure of competition, Harvard University Press.
2. Arulampalam, M. S. , Maskell, S., Gordon, N., and Clapp, T. (2002) "A Tutorial on Particle Filters for Online Nonlinear/Non-Gaussian Bayesian Tracking", by IEEE Trans. on Signal Processing, Vol 50, No. 2, Feb2002.
3. J. Burgoon and D. Buller, "Interpersonal deception: Ill effects of deceit on perceived communication and nonverbal behavior dynamics," Journal of Nonverbal Behavior, vol. 18, no. 2, pp. 155–184, 1994.
4. "Linguistic inquiry and word count." [Online]. Available:http://www.liwc.net/
5. Norman P, Boer H, Seydel E.R. 2005. Protection motivation theory. Predicting Health Behaviour. Open University Press, Berkshire, UK.
6. HAOJIN ZHU1 (Member, IEEE), SUGUO DU2, MUYUAN LI1 (Student Member, IEEE),AND ZHAOYU GAO1 (Student Member, IEEE), VOLUME 1, NO. 1, JUNE 2013
7. Rebecca Lefebvre, Kennesaw State University,1000 Chastain Road, MD 2201,Kennesaw, GA 30144,InfoSecCD'12, October 12 - 13 2012
8. R. Chandramouli,Department of Electrical and Computer Engineering, Stevens Institute of Technology Hoboken, NJ, USA, 978-0-615-51608-0/11 ©2011 EWI