# DETECTION AND PREVENTION OF BOTNET AND SYBIL ATTACK IN SOCIAL MEDIA

[1] Ms.P.Suganthi
[1]Assistant Professor
[1]Computer Science and Engineering,
[1]Sri Sairam Institute of Technology, Chennai, India

*Abstract : A botmaster is a person who operates the command and control of botnets for remote process execution. The botnets are typically installed on compromised machines via various forms of remote code installation. Botmasters have started to invade SOCIAL MEDIA (facebook, twitter, youtube ) by spamming, stealing private data through more flexible C&C channels. Since relentless spammers exploit the established trust relationships between account owners and their friends to efficiently spread malicious spam, timely detection of compromised accounts are quite challenging now-a-days. Here we propose a set of social behavioral features that can effectively characterize the user's social activities on facebook. The validation of the efficacy of these behavioral features by collecting and analyzing real user click streams in a facebook website to identify the compromised accounts is done . It evaluates the capability of the social behavioral profiles in distinguishing different facebook users and the proposed system shows that social behavioral profiles can accurately differ from individual facebook users and detect compromised accounts.*

*IndexTerms - Botmaster, Botnet, C&C channels, click streams, spamming, compromised account, behavioural features.*

## I. INTRODUCTION

As mentioned before, usage of FB mainly is wide-spread. There are many features in FB like Profile Picture loading, Message sharing, Reading Newsfeeds etc. In these profile picture can be morphed and used for other defective purposes. Wrong messages from an innocent account can be sent by hacking or through enabling botnet attacks through C&C channels.

Botnet attack in Facebook: Koobface ultimately attempts, upon successful infection, to gather login information for Facebook, Skype, and other social media platforms, and any sensitive financial data as well. It is not about creating fake account but it uses compromised computers to build a peer-to-peer botnet. A compromised computer contacts other compromised computers to receive commands in a peer-to-peer fashion. The botnet is used to install additional pay-per-install malware on the compromised computer and hijack search queries to display advertisements. Its peer-to-peer topology is also used to show fake messages to other users for the purpose of expanding the botnet.

Koobface originally spread by delivering Facebook messages to people who are "friends" of a Facebook user whose computer had already been infected. Upon receipt, the message directs the recipients to a third-party website (or another Koobface infected PC), where they are prompted to download what is purported to be an update of the Adobe Flash player. If they download and execute the file, Koobface can infect their system. It can then commandeer the computer's search engine use and direct it to contaminated websites.

Sybil Attack in Facebook:In a Sybil attack, the attacker subverts the reputation system of a peer-to-peer network by creating a large number of pseudonymous identities, using them to gain a disproportionately large influence. A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically. As of 2012, evidence showed that large-scale Sybil attacks could be carried out in a very cheap and efficient way in extant realistic systems such as BitTorrent Mainline DHT.

An entity on a peer-to-peer network is a piece of software which has access to local resources. An entity advertises itself on the peer-to-peer network by presenting an identity. More than one identity can correspond to a single entity. In other words, the mapping of identities to entities is many to one. Entities in peer-to-peer networks use multiple identities for purposes of redundancy, resource sharing, reliability and integrity. In peer-to-peer networks, the identity is used as an abstraction so that a remote entity can be aware of identities without necessarily knowing the correspondence of identities to local entities. By default, each distinct identity is usually assumed to correspond to a distinct local entity. In reality, many identities may correspond to the same local entity.

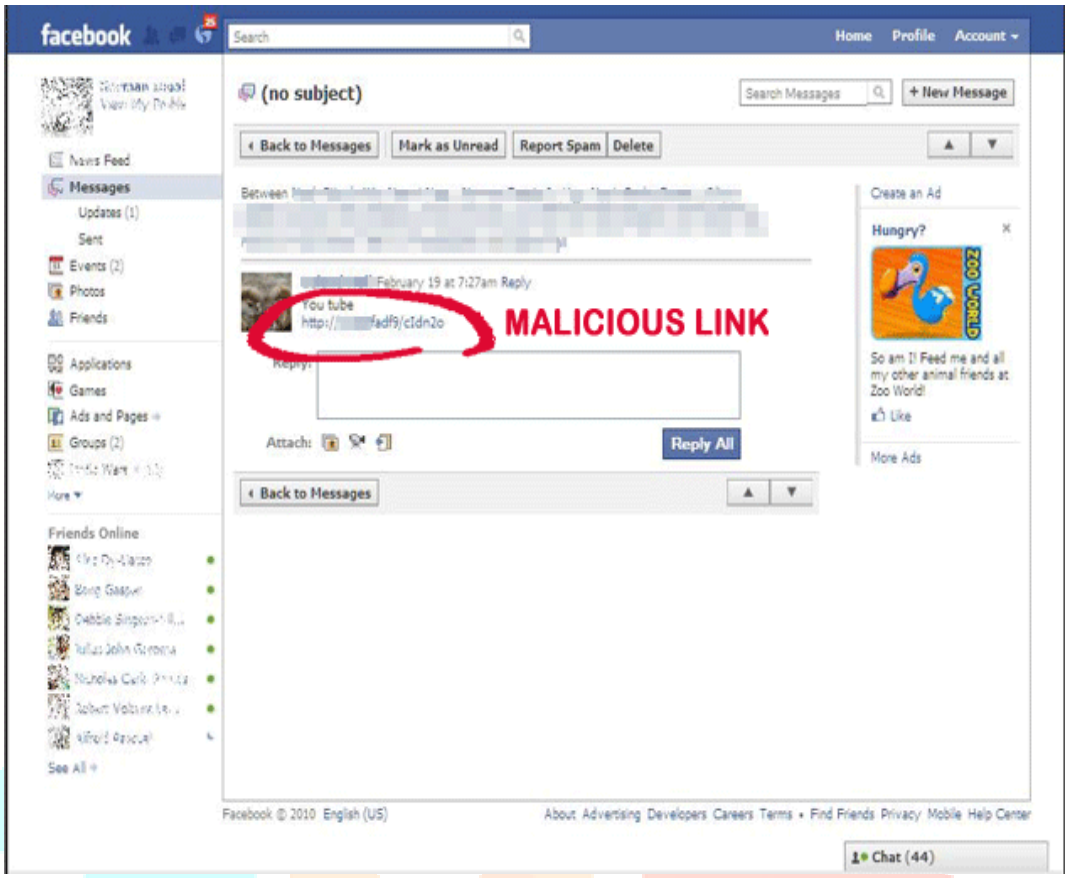


Fig 1: Attack in facebook

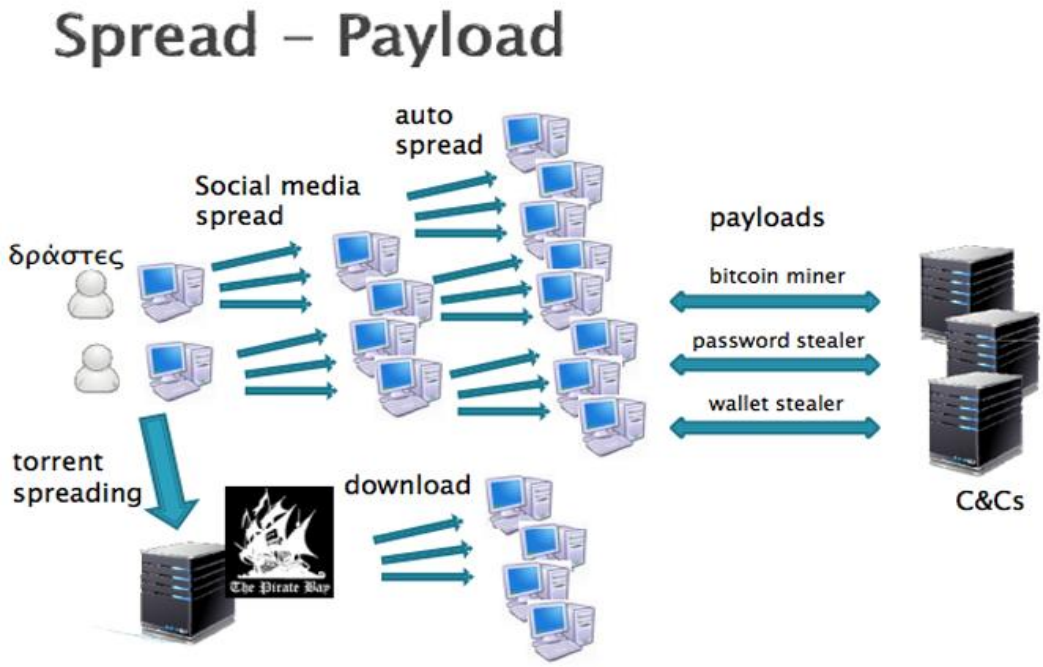


Fig 2: Botnet attack

**EXAMPLE:**

A notable Sybil attack (in conjunction with a traffic confirmation attack) was launched against the Tor anonymity network for several months in 2014 by unknown perpetrators. Many in the network security community suspect the NSA/CIA to be responsible for the attack, and some speculate that the attack may have been connected to the investigation into the Silk Road website.

## II. DESCRIPTION

### A. ALGORITHM DESCRIPTION:

Algorithm used : Spiral Credence Propagation

Spiral credence propagation is a dynamic programming approach to answering conditional probability queries in a graphical method. Given some subset of the graph as evidence nodes(observed variables E),compute conditional probabilities on the rest of the graph(hidden variables X).Spiral Credence gives exact marginal's when the graph is a tree(ie.has no loops),but only approximates the true marginals in loopy graphs

.

IDEA: Spiral Credence works by peer-pressure: a node X determines a final credence distribution by listening to its neighbours.Evidence enters the network at the observed nodes and propagates throughout the network.

Adjacent nodes exchange messages telling each other hoe to update beliefs, based on priors, conditional probabilities and evidence. We keep passing messages around until a stable belief state is reached (if ever).Credence Propagation may not give exact results on spiral graphs, but we use it anyway: iterate until convergence. The marginal's are often good approximations to the true marginals found by the junction tree algorithm. If credence propagation does not converge, it may oscillate between belief states.

### B. SYSTEM ANALYSIS:

#### 1. Existing System:

Existing system approaches involve account profile analysis and message content analysis (e.g. embedded URL analysis and message clustering). It classifies users based on their behavior: Extroversive or introversive behaviors. Extroversive behaviours, such as uploading photos and sending messages result in visible imprints to one or more users; introversive behaviours, such as browsing other users' profiles and searching in message inbox, however, do not produce observable effects to other users. It decides based on user's behaviour profile during a training phase (consistency check), whether the user's account is compromised. It is more straightforward to detect the compromisation of an inactive account because it can simply employ the existing solutions, such as checking its posting message behaviour and message content for anomaly detection. However, the various drawbacks are, the users' privacy is not effective and scalable in the existing system. Incomplete User Behavior Profiles. Varying click stream patterns of the users. (Sometimes attackers and the normal users have same patterns which will be untraced).This method assumes that cyber criminals cannot easily obtain target users' online social behaviour patterns. However, if more arduous hackers compromise the physical machines that users own, they are able to learn their social behaviour patterns and mimic the authentic users' social behaviours to avoid this detection method. It is hard to trace the behaviour patterns of users who access account via APIs, where this method may not be applicable.

#### 2. Proposed System:

In the proposed system, the user behaviour is traced by providing an additional option Usertype (chatter, newsfeeder, requester, profileview) in Facebook. By providing, this option the user behaviour can be analysed accurately and a graph will be generated based on the user's activity. So, when a botnet compromise the user's facebook account, according to the botnet's activity a graph will be generated. The spiral credence propagation, compare both the graphs, when they mismatch, the facebook account will be logged out immediately, and a onetime password will be generated and will be sent the user's mobile phone. The account will be logged in only after entering the one time password.

### C. IMPLEMENTATION

Unlike the normal Facebook, there is a new feature introduced in this proposed system by using SPIRAL CREDENCE PROPAGATION where user behaviour is tracked and if there is a difference in user behaviour, that is, it finds the difference between botnet behaviour or Sybil attack and user behaviour. It sends OTP to the user mobile number which is provided in the Facebook. A new feature with login called as behaviour which will contain the feature which user uses the most in Facebook is introduced . It can be like chatter, requester, newsfeed reader etc.

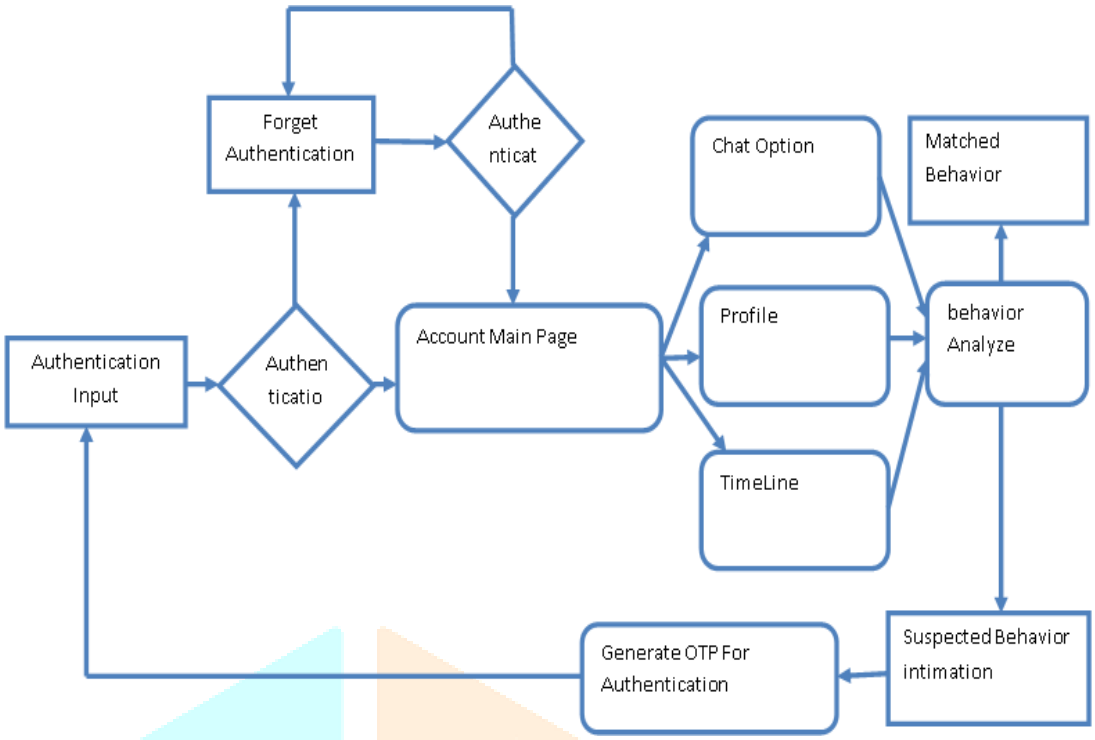


Fig 3: Behaviour change intimation

**D. MODULE DESCRIPTION:**

**1.Profile update and detection of discrepancies:**

This is the initial module where the user details in Facebook is filled. Phone number is a mandatory field in this profile. Phone number is the field through which security in our profile is enhanced. When there is a change or edit in phone number field, automatically OTP will be generated to the previous mobile number. This helps to find out if the person logged into the id is the original user.

**2.User behaviour analysis and graph creation:**

This module includes the Registration of the user,chatting with the friends of the user and requesting other users. It consist of Behavior option which should be selected by the user during behavior change. Continuous Monitoring of the account is possible. Different actions of the user is analyzed. Graph is created based on SPIRAL CREDENCE PROPAGATION. Spiral credence propagation is a dynamic programming approach for answering conditional probability queries in a graphical method. Spiral Credence works by peer-pressure: a node determines final credence distribution by listening to its neighbours. Adjacent nodes exchange messages telling each other how to update credence based on conditional probabilities and evidences.This module involves User-friend chat.

**3. User behaviour and bot behaviour comparison:**

It also compares the request given by the user and the current requests given based on the Usage Database. It continuously compares the current action of the user in Facebook and the behavior option selected by the user during registration. It checks the count value of other pages viewed by the user. It checks for SYBIL ATTACKS and protects the user account. Sybil attack- An adversary creates multiple bogus identities to compromise account of the user. After being compromised, the behavior of the account changes which is compared with the previous behavior of the user using behavior database and prevention steps are carried out.

**4. Account restoration and security enhancement**:

This deals with Security enhancement where alert is generated after the discovery of attack in the account. It analyzes and checks through dissimilar and unwanted requests to users. After analyzing the bot requests in the account, alert message with OTP is sent to user device. It also analyzes unwanted message sharing and deviation from behavior selected. It temporarily blocks the account after finding discrepancy in user behavior. Original user logs into the account again using OTP generated . This prevents Sybil and Bot attacks.

## III. RELATED WORKS

Michael Sirivianos [7] introduces a new tool in the hands of OSN operators, known as SybilRank . It relies on social graph properties to rank users according to their perceived likelihood of being fake (Sybils). SybilRank is computationally efficient and can scale to graphs with hundreds of millions of nodes. YoramBachrach [5] show how user's activity on Facebook relates to their personality, as measured by the standard FiveFactorModel. The dataset consists of the personality profiles and Facebook profile data of 180,000 users. They examine correlations between users' personality and the properties of their Facebook profiles such as the size and density of their friendship network, number of uploaded photos, number of events attended, number of group memberships, and number of times user has been tagged in photos. Their results show significant relationships between personality traits and various features of Facebook profiles. They show how multivariate regression allows prediction of the personality traits of an individual user given their Facebook profile. Christopher Kruegel's [8] approach uses a composition of statistical modelling and anomaly detection to identify accounts that experience a sudden change in behavior

## IV.SYSTEM STUDY

### FEASIBILITY STUDY

The basic objective is to provide security. In the present generation usage of Social media is global and extensive. And as the usage is in excess hence there is a critical need for security as we come across plenty of problems due to social media usage.

- TECHNICAL FEASIBILITY
- ECONOMIC FEASIBILITY
- LEGAL FEASIBILITY
- RESOURCE FEASIBILITY

Common Factors:

- Technical Feasibility:

The implementation of this concept requires Visual studio to develop computer programs for Microsoft Windows. It uses Microsoft software development platforms such as Windows API, Windows Forms, Windows Presentation Foundation etc. It also requires programming in .NET which runs only on Windows Platform. Some tools are not present in Java hence we use .NET for development.

- Economic Feasibility:

It is not that much costly as the front-end is .NET which already exists and we use SQL and Visual Studio for back-end which is also commonly used.

- Legal Feasibility;

It can become legal as it is the modification of already existing legalized Face book application.

- Resource Feasibility;

There is existence of enough resource for development . So resource availability is extensive.

## V.CONCLUSION

As social media is being used in day-to-day life, there is an instant need for security. Hence, the proposed system provides end to end security in order to avoid Sybil and botnet attacks through behaviour analysis. Comparison is based on graph and accurate results are achieved. The difference between hacker behaviour and normal user behaviour is successfully found in case of the account being compromised. New options are proposed in facebook as per user convenience. They are proposed in a way, such that it do not appear as a hindrance to the innocent users

**REFERENCES**

[1] *250,000 Twitter Accounts Hacked*. [Online]. Available:http://www.cnn.com/2013/02/01/tech/social-media/twitter-hacked,accessed Sep. 2013.RUAN *et al.*: PROFILING ONLINE SOCIAL BEHAVIORS FOR COMPROMISED ACCOUNT DETECTION 187

[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. ACMWeb Sci. Conf. (WebSci)*, Evanston, IL, USA, 2012, pp. 24–32.

[6] F. Benevenuto, T. Rodrigues, M. Cha, and V. Almeida, "Characterizinguser behavior in online social networks," in *Proc. 9th ACM SIGCOMMConf. Internet Meas. Conf. (IMC)*, Chicago, IL, USA, 2009, pp. 49–62.

[7] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, "Aiding the detectionof fake accounts in large scale social online services," in *Proc. 9thUSENIX Conf. Netw. Syst. Design Implement. (NSDI)*, San Jose, CA,USA, 2012, p. 15.

[8] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "COMPA: Detectingcompromised accounts on social networks," in *Proc. Symp. Netw.Distrib. Syst. Secur. (NDSS)*, San Diego, CA, USA, 2013.

[9] H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary, "Towardsonline spam filtering in social networks," in *Proc. Symp. Netw.Distrib.Syst. Secur. (NDSS)*, San Diego, CA, USA, 2012.

[10] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, "Detectingand characterizing social spam campaigns," in *Proc. 10th ACMSIGCOMM Conf. Internet Meas. (IMC)*, Melbourne, VIC, Australia,2010, pp. 35–47.