Sybil Attack and its Proposed Solution

Hardik Jhaveri
B.E. [I.T.]
Mumbai University

Harshit Jhaveri
B.Sc[I.T.], MCA
Mumbai University

Dhaval Sanghavi
B.E. [C.S.]
Mumbai University

ABSTRACT

Social engineering, in terms of information security, refers to manipulation of people into performing actions or divulging information. A type of trick for the purpose of gathering of information, fraud, or system access, it differs from a traditional "con. "Social engineering" is define as an act of psychological manipulation which is also associated with the social sciences, but its usage has caught computer and information security professionals.

Keywords

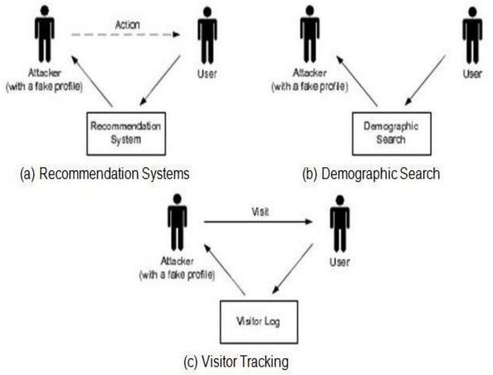
Reverse Social Engineering, Sybil Attack, Social Engineering

1. INTRODUCTION

In a reverse social engineering attack, the attacker does not start contact with the victim. Rather, the victim intiate the contacts. Because of this, trust is established between the victim and the attacker as the victim is the entity that established the relationship. In this report, we first present the user study on reverse social engineering attacks in social networks. Reverse social engineering attacks are feasible and effective in practice. Social networking sites such as Facebook and Twitter are arguably the fastest growing web-based online services today. Facebook, has been reporting growth rates as high as 3% per week, with more than 410 million registered users as of March 2010. Many users appreciate social networks because they make it easier to meet new people, search old friends, and share multimedia artifacts such as videos and photographs. Clearly, social networks are critical applications with respect to the security and privacy of their users. In fact, the large quantity of information published, on the user profiles is increasingly attracting the attention of attackers. This report presents a user study on how attackers can abuse some of the features provided by online social networks with the aim of launching automated reverse social engineering attacks. We present three most important attacks, recommendation-based, visitor tracking-based, and demographics-based reverse social engineering.

2. TYPES OF ATTACK

In the first attack, the aim is to exploit the recommendations made by the social network to promote the fake profile of a user. In the second tracking attack, the aim is to trigger the target's curiosity by browsing her profile page. Finally, in the third-based attack scenario, the attacker attempts to approach the victims by copying fake demographic with the aim of attracting the attention of users with similar preferences.



(a) Recommendation Systems

(b) Demographic Search

(c) Visitor Tracking

3. CHARACTERISTICS OF ATTACKS

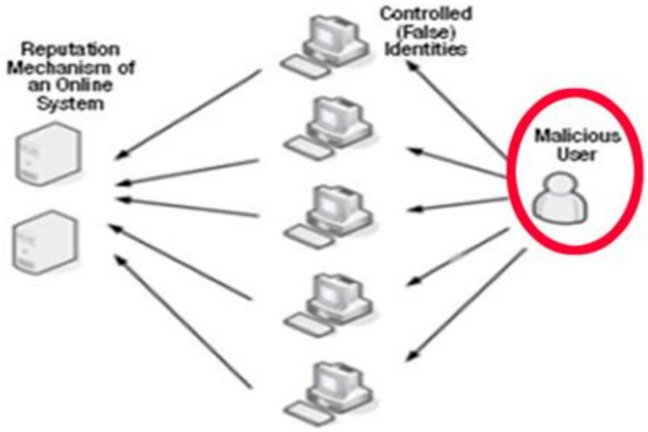
Targeted/Untargeted: In a targeted attack, the attacker focuses on a particular user. In an un-targeted attack, the attacker is interested in reaching users.

Direct/Mediated: In a direct attack, the action of the attacker is visible to the targeted users. Mediated attacks, follow a two-step approach in which the baiting is collected by an agent that is then responsible for propagating it to the users.

Sybil attack: In this attack, the attacker creates multiple fake identities and uses them to gain a large influence

4. SYBIL ATTACK

In a Sybil attack, an adversary creates a large number of forging/fake/pseudonymous identities (also named Sybil identities), and since all Sybil identities are controlled by the adversary, he can maliciously introduce a considerable number of false opinions into the system, and making decisions benefiting himself/herself. Essentially, Sybil attacks break and manipulate the trust mechanism behind peer-to-peer systems. For a better understanding of what a Sybil attack is, here are examples. First, in some distributed systems, critical resources are assigned based on the voting results of participants: usually, only the node that has received the highest number of votes can access the resources. If an attacker unlegally creates a large number of Sybil identities, then the dreary can proportion more resources by instructing the fake identities to vote in certain ways.. Since votes are collected indirectly, it is hard to detect the illegitimate votes. Second example comes from an application of sensor networks called 'pervasive temperature monitoring. Each sensor measures surrounding temperature, and move to sink node, which collects the data. The sink node calculate the average temperature can be computed.. Our third example comes from a Facebook voting application. If an malicious creates many identities, he can easily change the overall popularity of an option by providing plenty of false praise, or bad-mouthing of the option through Sybil ids. Since the wrong opinions of the Sybils may essentially change the final decision of any system, the research works on Sybil defense techniques hold the most important position. Various Sybil attacks are as follows


Reputation Mechanism of an Online System
Controlled (False) Identities
Malicious User

4.1 Insider Vs Outsider

Whether an attack is an insider or outsider directly determines the capability of the attacker, and the hardness of launching a Sybil attack. The insider attacker holds at least one legitimate identity and claims that he receives certain data, by using the fake identities. However, for an outsider, she is any illegitimate entity; before launching a Sybil attack, he must first access the system. However, distributed systems typically employ some kind of authentication to prevent illegitimated access, such as a password for entering, or data encryption. They need to understand the mechanism of the system prior of launching Sybil attacks. Due to this, distributed systems are more vulnerable to inside attackers.

4.2 Selfish Vs Malicious

For security-related problems, there are two different types of attackers: either selfish or malicious. Selfish attackers manipulate the false data, while malicious attackers attempt toundermine a system. Whether an attacker is selfish or malicious is usually determined by the different types of targeted distributed system and final attacking effects. For However, if other users can used the resource with lower probability, then he is selfish. Since malicious attacks have more serious effects, it is of great importance to defend against potentially malicious attacks than those that are potentially selfish.

4.3 Directed Vs Undirected

How Sybil nodes communicate with honest nodes is also a significant consideration during the designing of Sybil defense mechanisms. The attacker can communicate with an true node by using one of her Sybil identities, or he can use only her real identity to communicate with others, and route the Sybil data. For the attackers, the easiness of direct communication with honest nodes directly influences the success of attacking, and whether honest users can see through the attack. Tthe attackers with more directed communications are harder to detect

4.4 Busy Vs Idle

All Sybil identities can participate in a distributed system simultaneously, or only some of them can work, while others are in a state that is idle. The selection of these two schemes is determined by how cheap it is to obtain an identity. If the attacker can easily get lot of fake identities, having some idle Sybil nodes could make them much more real, since an true node may leave the system multiple times. However, the power of Sybil attacks results from the quantity of the identities. If large number of identities is difficult to obtained, the attacker has to use all of them in order to launch a successful attack.

5. RELATED WORK

Social engineering attacks are well-known in practice as well as in literature. Social engineering targets human weaknesses instead of vulnerabilities in technical systems. Automated Social Engineering (ASE) is the process of automatically executing social engineering attacks. Spamming and phishing can be seen as a very simple social engineering form. A very common problem on social networks is that it is harsh for users to judge if a friend request is trustworthy or not. Thus, users are quick in accepting invitations from people they don’t know.. More cautions users can be tricked by requests from adversaries that impersonate friends. Unfortunately, once a connection is made, the attacker typically has access to all information on the victim’s profile. Beside, users who receive messages from fake friends are much more likely to act upon such message, for example, by clicking on links. In contrast to active social engineering that requires the attacker to establish contact or a touch with the victim, in a reverse social engineering attack, it is the victim that contacts or touches the attacker. We are not known of any previous reports or studies on reverse social engineering attacks in online social networks. The results of this paper shows that reverse social engineering is a threat, and that it is feasible in practice

6. PROPOSED SOLUTION

Our entire research deals with reverse social engineering attacks. Initially we studied about Social Engineering and its types. This was followed by an extensive study on Reverse Social Engineering attacks and an analysis on how reverse social engineering attacks are committed on social networking sites. Then, relevance of social engineering attacks on peer to peer systems, also called as Sybil Attack was included. Moving on to the actual topic of Reverse Social Engineering attacks on Social Networking Sites, we have come up with a fact that most of these attacks done by the attacker are done through fake/fraudulent social networking profiles. Thus one way to prevent such attacks is to find out and alert the victim of profiles being fake/false. Thus our solution to these attacks mainly involves the process of finding out fake/fraudulent profiles on social networks. To do this, we have to perform an extensive data mining process on profiles of peers of the victim. The entire procedure of finding out fake profiles is divided in three modules:

6.1 Extracting the Display Image

Once these pictures are extracted, they are searched on Google through picture pattern searching and matching of Google. It is expected that if most of the images are found in Google search, then the probability of the profile being fake is high. This is because images on Google are public images. Normally, attackers will not put their own images, or images of their peers as a picture of a fake social network profile. Thus we use this hypothesis as the most important factor to consider a profile to be fraudulent. Note-The attacker may not have kept his own photo on the profile, or a public image but he might have kept a photo of say a hotel or a statue which he might have clicked by himself. Then in such cases the Google image search will not show any match. Thus the probability of a fake profile being fake would be low. To overcome such a problem, we need to consider some more information and activities of that profile to consider it as a fake one.

6.2 Data Mining Information

After performing a check on the available pictures of the profile, we move on to extraction of personal information of the user from his profile. That includes details like – school name, work place, college name, home town, city, spouses, cousins, email id, contact number, etc. Once we extract these information's, we compare them with that of the victim to find out the relevance of the fake profile user with the victim. If there is relevance, e.g. both of them studied in the same school then, probability of that profile being fake is less. But normally attackers don't fill in all the details or just fill fake details in order to complete the process of creating a new profile. Thus using this hypothesis we can find out the probability of relevance of the fake profile with that of our victim

6.3 Profile Activity Analysis

The activity log of the fake profile, that includes his wall posts on his own wall, his comments on his pictures and on other's peoples pictures, his reply on wall posts etc. The higher activity the profile owner has, the lower is the possibility of that profile being fake. The hypothesis is that normally fake profiles are created to perform an attack on the victim and not to socially interact with multiple people as it is time consuming and irrelevant. Thus again this hypothesis is used to classify the profile as real or fake. The entire aim of our solution is to create software that extracts data of the victim and compares it with all its friends and incoming friend requests. This system will act as a classifying system which will notify the user whether the incoming friend request is from a real friend or a fake one. This is just a classifying system, i.e. the user will be told that the incoming request has been verified and the profile has been classified into real or fake. Here, the user will ultimately decide whether to accept the request or not.

7. CONCLUSION

Hundreds of millions of users are registered to social networking sites and regularly use these features to stay in touch with friends. To make suggestions, social networking sites often mine the data that has been collected about the users that are registered. For example, the fact that a user looks up an e-mail address might be assumed to indicate that the user knows the person who owns that e-mail account.. Peer-to-peer systems play an ever-increasingly important part of our daily lives. However, most of the peer-to-peer systems are vulnerable to Sybil attacks. In order to design more efficient and practical Sybil defenses, we write this report. We first give the definition of Sybil attacks, and provide the classification of Sybil attacks. Then, we give several realistic systems which are vulnerable to Sybil attacks. After that, defense mechanisms and their corresponding strengths and weaknesses were discussed. Unlike other surveys, we describe these mechanisms according to anti-Sybil approaches' developing Stages. Our results show that RSE attacks are a feasible threat in real-life, and that attackers may be able to attract a large numbers of legitimate users without actively sending any friend request. The experiments we have conducted suggest that suggestions and friend-finding features made by social networking sites may provide an incentive for the victims to contact a user if the right setting is created .We hope that this paper will increase awareness about the real-world threat of reverse social engineering in social networks and will encourage social network providers to adopt some countermeasures.

8. ACKNOWLEDGEMENT

We would like to thank our parents Mr. Ketan Jhaveri, Mrs. Bina Jhaveri, Mr. Rohit Sanghavi,Sudha Sanghavi for their love, support and encouragement during all times and for always believing in us.

9. REFERENCES

[1] H. Yu, M. Kaminsky, P. Gibbons, and A. Flaxman, "Sybilguard: defending against sybil attacks via social networks," in *Proc. of ACM SIGCOMM*, vol. 36, no. 4, 2006, pp. 267–278.

[2] H. Yu, "Sybil defenses via social networks: a tutorial and survey," *SIGACT News*, vol. 42, no. 3, pp. 80–101, 2011.

[3] B. Viswanath, A. Post, K. Gummadi, and A. Mislove, "An analysis of social network-based sybil defenses," in *Proc. of ACM SIGCOMM*, vol. 40, no. 4, 2010, pp. 363–374.

[4] X. Zheng, Y. Lai, K. Chow, L. Hui, and S. Yiu, "Sockpuppet detection in online discussion forums," in *Proc. of IEEE IIH-MSP*, 2011, pp. 374–377.

[5] L. Page, S. Brin, R. Motwani, and T. Winograd, "The PageRank citation ranking: bringing order to the web," *Technical report, Stanford University*, 1999.

[6] J. Golbeck, B. Parsia, and J. Hendler, "Trust networks on the semantic web," *Cooperative Information Agents VII*, pp. 238–249, 2003

[7] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *Proc. of ACM IPSN*, 2004, pp. 259–268.