Sybil Attacks VS Identity Clone Attacks in Online Social Networks

Lei Jin, Xuelian Long, Hassan Takabi, James B.D. Joshi

School of Information Sciences
University of Pittsburgh, Pittsburgh, PA, USA
{lej17, xul10, hat26, jjoshi}@pitt.edu

Abstract. *Sybil attacks* and *Identity Clone attacks* (also known as *Profile Cloning attacks*) have become significant security and privacy concerns for online social network (OSN) systems integrated with reputation or evaluation mechanisms. In both attacks, adversaries first create multiple identities and then launch attacks to compromise reputation or evaluation mechanisms in OSN systems. In this paper, we discuss and distinguish these two attacks. The comparisons between them are presented based on pre-requirements, network topology and attack impacts.

Keywords: Sybil Attack, Identity Clone Attack, Online Social Networks

1 Introduction

Some Online social networks (OSN) systems, such as *YouTube* and *Digg*, are integrated with reputation and/or evaluation mechanisms. One of the striking features in these OSN systems is that the popularity and the value of a resource, such a video in *YouTube* and a piece of News in *Digg*, are driven by users' participations and feedbacks. However, this feature is also attractive to adversaries who have incentives to distort the popularity and value of the resource. Generally, adversaries can launch *Sybil attack* or *Identity Clone attack* to achieve their malicious purposes. *Sybil attacks* [1] focus on creating multiple online user identities (*Sybil* identities) and try to achieve malicious results through these identities. In an *Identity Clone attack* (also called *Profile Cloning attack*) [2, 3], an adversary first creates similar or even identical profiles to impersonate victims in an OSN system. He then distorts the reputation and the value of a resource through the network involving faked profiles.

Sybil attacks and *Identity Clone attacks* look somehow similar in appearance since both attacks need to create a number of online identities, and use these identities to compromise the reputation and evaluation mechanisms in OSN systems. These similar attack patterns could confuse administrators of OSN systems. As a result, administrators may have difficulties in distinguishing between *Sybil attacks* and *Identity Clone attacks* and they may not deploy appropriate and efficient defense approaches against them. Therefore, it is vital for them to first distinguish between *Sybil attacks* and *Identity Clone attacks*. In this paper, we analyze and compare *Sybil attacks* and *Identity Clone attacks* in OSN systems based on their characteristics. To

the best of our knowledge, our work is the first attempt to identify the differences between a *Sybil attack* and an *Identity Clone Attack*.

2 Comparisons between Sybil Attack and Identity Clone Attack

In this section, we present the distinguishing characteristics of a *Sybil attack* and an *Identity Clone attack* based on the pre-requirements, network topologies and impacts of the attacks.

2.1 Pre-Requirements of Attacks

To launch a *Sybil attack* on an OSN system, an adversary needs to create multiple identities. According to our earlier survey [4], most OSN systems require a user to choose a username or input his e-mail address during the account registration process. This result indicates that adversary needs to have multiple unique usernames or a huge number of e-mail addresses for launching the attack. Thus, the adversary also needs to compromise this restriction in the registration process, in order to create many identities automatically.

To launch an *Identity Clone attack*, an adversary also requires a number of unique usernames and e-mail addresses for creating identities in an OSN system. Additionally, the knowledge of a victim (identity that is cloned) is another pre-requirement in an *Identity Clone attack*.

2.2 Network Topology

As shown in Figure 1, when a *Sybil attack* is present, a social network graph can be conceptually divided into two parts: one consisting of all genuine identities and the other consisting of all *Sybil* identities. The link connecting a genuine node to a *Sybil* node is called an *attack edge* [5].

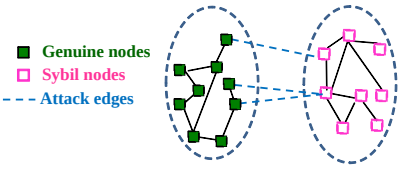

Figure 1. A network of a *Sybil attack*

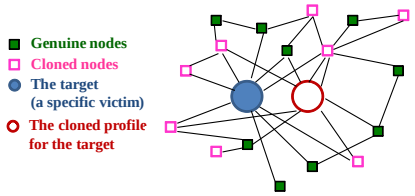

Figure 2. A network of an *Identity Clone attack*

In the network of an *Identity Clone attack*, there are two types of nodes: genuine nodes and cloned nodes. For example, in Figure 2, a large solid sphere is the target node while a large hollow sphere is the cloned identity created by an adversary and impersonating the target. The small solid squares are the other genuine nodes and the hollow squares are the rest of the cloned nodes created by the adversary to impersonate the target's friends or potential friends.

2.3 Attack Impacts

A *Sybil attack* can be used to affect the popularity, reputation, value and other characteristics of resources in OSN systems by using *Sybil* nodes. An adversary can boost invaluable resources and resource providers who have bad reputations. He can also downgrade valuable resources and reputable resource providers. In addition, the adversary can launch spam attacks by requesting the *Sybil* identities to propagate malicious messages to their neighbor nodes. Similar to *Sybil attacks*, *Identity Clone attacks* can affect the popularity, reputation, value of resources in OSNs using fake profiles. Additionally, such attacks can also influence the choices made by victims' friends using the trust built in friendships.

3 Conclusions

As the value of OSN systems is widely recognized, the incentive to attack such systems is rapidly growing. In this paper, we analyze two attacks: *Sybil attacks* by creating *Sybil* nodes and *Identity Clone attacks* by creating cloned profiles. Both attacks require adversaries to create multiple identities and focus on distorting reputation and/or evaluation mechanisms in OSN systems. In order to distinguish these two attacks, we have also discussed and compared their characteristics. We have demonstrated that the pre-requirements, network topology and attack impacts can be distinguished. We believe that researchers and administrators of OSN systems could use these different characteristics to understand *Sybil attacks* and *Identity Clone attacks* more comprehensively and then have more confidence to deploy appropriate defense approaches against them. As future work, we plan to develop a defense framework that works for both *Sybil attacks Identity Clone attacks* based on characteristics and differences we proposed in this paper. We will also validate our defense approaches in a real OSN system.

References

1. Newsome J., Shi E., Song D., Perrig A.: The sybil attack in sensor networks: analysis & defenses. In: 3rd International Symposium on Information Processing in Sensor Networks, Berkeley, California, USA (2004)
2. Bilge L, Strufe T., Balzarotti D., Kirda E.: All your contacts are belong to us: automated identity theft attacks on social networks. In: 18th international Conference on World wide web, Madrid, Spain (2009)
3. Jin L., Takabi H., Joshi J. B. D.: Towards active detection of identity clone attacks on online social networks. In: 1st ACM Conference on Data and Application Security and Privacy, San Antonio, TX, USA (2011)
4. Jin L., Takabi H., Joshi J. B.D.: Analyzing Security and Privacy Issues of Using E-mail Address as Identity. Int. J. Information Privacy, Security and Integrity, Vol. 1, No. 1 (2011)
5. Yu H., Kaminsky M., Gibbons P. B., Flaxman A. D.: SybilGuard: defending against sybil attacks via social networks. IEEE/ACM Trans. Networking, Vol.16, No. 3, pp. 576--589 (2008)