Detecting In-Situ Identity Fraud on Social Network Services: A Case Study on Facebook

[1]Shan-Hung Wu, [2]Man-Ju Chou, [3]Chun-Hsiung Tseng, [2]Yuh-Jye Lee, and [4]Kuan-Ta Chen*

[1]Dept. of Computer Science, National Tsing Hua University
[2]Dept. of Computer Science, National Taiwan University of Science and Technology
[3]Dept. of Information Management, Nanhua University
[4]Inst. of Information Science, Academia Sinica

ABSTRACT

In this paper, we propose to use a continuous authentication approach to detect the *in-situ identity fraud incidents*, which occur when the attackers use *the same devices and IP addresses* as the victims. Using Facebook as a case study, we show that it is possible to detect such incidents by analyzing SNS users' browsing behavior. Our experiment results demonstrate that the approach can achieve reasonable accuracy given a few minutes of observation time.

1. OVERVIEW

Many people use Social Networking Services (SNSs) like daily, and link a lot of personal and sensitive information to their SNS accounts. The information generally includes friend lists, feeds from friends, non-public posts/photos, private interactions with acquaintances (such as chats and messages), and purchased apps/items. The obvious value of such information makes SNS accounts one of the most targeted online resources by hackers. SNS sites have made significant efforts to prevent identity fraud and protect users' privacy. For example, Facebook records the regular IP addresses and devices used by each account. If an unusual IP address or device is used to log in to an account, the user is asked to answer some secret questions [1] or enter a security code sent to the account owner's mobile device [2] in order to verify if the login is authentic. Facebook also allows users to report account theft manually if they suspect their accounts have been compromised.

Despite all the efforts to prevent identity fraud, user privacy can be compromised by another form of breach called *in-situ identity fraud*—unauthorized, stealthy use of SNS accounts by attackers using the same device and network connection as the account owners. Different from other forms of identify fraud, anyone can perform in-situ identity fraud without any technology hacks. For example, anxious parents may use their children's SNS accounts to spy on the children's social status; or husbands/wives may check their spouses' SNS accounts if they suspect infidelity. Similarly, colleagues, supervisors, friends, and siblings, may use acquaintances' accounts for different reasons when there is a chance.

In-situ identity fraud is widespread for a number of reasons. First, people tend to choose "yes" when the browsers on their own computers ask if they want to save their (SNS) passwords for automatic logins in the future. This is especially true when people use their mobile devices because inputting passwords is inconvenient [10, 7]. Mobile devices make in-situ identity fraud easy in other ways, as they can be physically accessed by acquaintances or strangers [11], and most of them are not locked by PINs [5]. In addition, many SNS sites use cookies to avoid the need for account authentication within a short period of time. For example, once logged into Facebook, a user does not need to log in again for up to 60 days [3]. Given the above drawbacks, if someone (usually an acquaintance) can access an SNS user's computer or mobile device, it is unlikely that he will need a technical background to obtain the information associated with the SNS account.

In this paper, we investigate the in-situ identity fraud problem in SNSs, and propose a continuous authentication approach [8, 9] that analyzes users' browsing behavior to detect such incidents. Using Facebook as a case study, we show that it is possible to detect this special type of attacks on SNS sites by analyzing users' browsing behavior, for example clicks on newsfeeds, friend lists, profiles, likes, messages, photos/videos, and comments. The results demonstrate that the proposed scheme can achieve more than 80% accuracy with a high degree of confidence within 2 minutes, and over 90% after 7 minutes of observation time.

2. DETECTION SCHEME

SNS services are not simply places for people to maintain their friend lists. They are more like platforms where people can engage various social activities, such as posting details of their own status, reading other users' comments on the news, chatting, and meeting new people. Some studies [4, 6] suggest that there is *no typical* user behavior pattern on a complicated, open platform like Facebook, as every user seems to behave differently on an SNS service. For example, some people use SNSs to satisfy their desire for self-promotion, so they spend most of their time sharing the

*Contact e-mail address: ktchen@iis.sinica.edu.tw

†This work was partly supported by National Science Council, National Taiwan University and Intel Corporation under Grants NSC101-2221-E-001-012-MY3, NSC102-2911-I-002-001, and NTU103R7501.

WWW'14 Companion, April 7–11, 2014, Seoul, Korea.
ACM 978-1-4503-2745-9/14/04.
http://dx.doi.org/10.1145/2567948.2577308.

latest information about their status and posting the latest photos/events. On the other hand, some people may want to make new friends online, chat with old friends, or spend time discovering new social games; and some may want to stalk certain other users.

In the context of in-situ identity fraud, an SNS user can be classified as fulfilling one of the following roles: 1) an *owner*, which means the person uses his own account; 2) an *acquaintance* (as a stalker), who uses the account of someone he knows; or 3) a *stranger* (as a stalker), who uses the account of a person he does not know. Intuitively, when owners check their Facebook newsfeeds, they should focus more on the latest information posted by friends and use the "like" or "share" function to interact with others. By contrast, when a stalker (either an acquaintance or a stranger) browses a newsfeed, he may be more interested in old information about the stalker and/or the account holder. Also, the stalker generally do not interact with others to avoid discovery by the account holder about the identity fraud. In summary, we believe that users' behavior varies in different roles for the following reasons:

- The way people treat familiar information (and information from close friends) would be different than the way they treat unfamiliar information.
- People in different roles have different intentions.
- To avoid detection by the account owners, stalkers tend to not make any interaction with others. Also, they may have limited time to commit in-situ identity fraud so their browsing behavior would be even more different.

We define the above differences in SNS users' browsing behavior as *role-driven behavioral diversity*, which serves the rationale behind the proposed detection scheme.

Figure 1 provides an overview of the detection scheme. After a user logs in with a stored credential or existing authentication cookies (Step 1), the SNS server monitors and records the user's actions for an *observation period* of n minutes, where n is a configurable parameter (Step 2). At the end of the observation period, the server extracts the features of the monitored session based on the recorded actions (Step 3). It then feeds the session features which characterize users browsing behavior, into a classification model (Step 4), which determines if the session owner is suspicious by predicting the label of the session (Step 5). If the predicted label is "stalker," the SNS server can challenge the user by asking secret questions or via a second channel, such as the account owner's mobile phone (Step 6). Alternatively, the server can implement a more sophisticated, but costly, detection scheme.

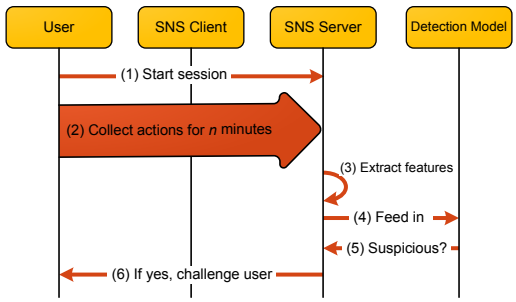

Figure 1: The flow chart of the detection scheme.

3. CONCLUSION

In this paper, we have proposed a low-cost continuous authentication scheme for SNSs that analyzes users' browsing behavior to detect in-situ identity fraud incidents. Using Facebook as a case study, we show that 1) the *role-driven behavioral diversity* property does exist; 2) the property can be exploited to design a low-cost detection scheme that is applicable to all users; and 3) the scheme is hard to evade and it renders a reasonable detection performance after an observation period of 2 minutes.

We believe that the in-situ identity fraud problem, which has not been widely studied, will become more critical in the future as people store increasing amounts of sensitive information online. In fact, the problem may also occur in email services like Gmail and Outlook; time management services like Google Calendar and Remember The Milk; and photo album services like Instagram. Asking users to authenticate themselves repeatedly during the use of the services is infeasible in practice due to usability issues. Thus, continuous authentication seems to be a reasonable way to prevent attacks of this kind.

4. REFERENCES

[1] Josh Constine. Facebook has users identify friends in photos to verify accounts, prevent unauthorized access. `http://www.insidefacebook.com/2010/07/26/facebook-photos-verify/`, 2010.

[2] Josh Constine. Facebook asks every user for a verified phone number to prevent security disaster. `http://techcrunch.com/2012/06/14/facebook-security-tips/`, 2012.

[3] Facebook. Removal of offline_access permission. `https://developers.facebook.com/roadmap/offline-access-removal/`.

[4] Keith Hampton. Social networking sites and our lives part 2: Who are social networking site users? `http://pewinternet.org/Reports/2011/Technology-and-social-networks/Part-2/Facebook-activities.aspx`, 2011.

[5] Ed Hansberry. Most consumers don't lock mobile phone via PIN. `http://www.informationweek.com/mobility/security/most-consumers-dont-lock-mobile-phone-vi/231700155`, 2011.

[6] Adam N Joinson. Looking at, looking up or keeping up with people?: motives and use of Facebook. In *Proc. of ACM CHI 2008*, pages 1027–1036, 2008.

[7] Paul Mah. Stored passwords add to mobile security risks. `http://www.itbusinessedge.com/cm/blogs/mah/stored-passwords-add-to-mobile-security-risks/?cs=47183`, 2011.

[8] Maja Pusara and Carla E Brodley. User re-authentication via mouse movements. In *Proc. of the ACM Workshop on Visualization and data mining for computer security*, pages 1–8, 2004.

[9] SJ Shepherd. Continuous authentication by analysis of keyboard typing characteristics. In *European Convention on Security and Detection*, pages 111–114, 1995.

[10] Credant Technologies. Phone data makes 4.2 million* brits vulnerable to ID theft. `http://www.credant.com/news-a-events/press-releases/69-phone-data-makes-42-million-brits-vulnerable-to-id-theft.html`.

[11] Roger Yu. Lost cellphones added up fast in 2011. `http://usatoday30.usatoday.com/tech/news/story/2012-03-22/lost-phones/53707448/1`, 2012.