Exploiting Online Social Behaviors for Compromised Account Detection

Haining Wang
University of Delaware
E-mail: hnw@udel.edu

Compromised accounts in Online Social Networks (OSNs) have been becoming more favorable than spam or sybil accounts to spammers and other malicious OSN attackers. These malicious parties exploit the well-established connections and trust relationships between the legitimate account owners and their friends to efficiently distribute spam ads, phishing links, or malware. Unlike dedicated spam or sybil accounts, which are created solely to serve malicious purposes, compromised accounts are originally possessed by benign users, and later hijacked by cyber criminals. While dedicated malicious accounts can be simply banned or removed upon detection, compromised accounts cannot be handled likewise due to potential negative impact to normal user experiences (e.g., those accounts may still be actively used by their legitimate benign owners). Major OSNs today employ IP geolocation logging to defend against account compromisation. However, this approach is known to suffer from low detection granularity and high false positive rate.

Therefore, account compromisation is posing a serious threat to users of Online Social Networks (OSNs). On one hand, relentless spammers exploit the rich social connections of compromised accounts and the established trust relationships between account owners and their friends to efficiently spread malicious spam messages. On the other hand, timely detection of compromised accounts is quite challenging due to the well established trust relationship between the service providers, account owners, and their friends. In this project, we will investigate the social behaviors of OSN users, i.e., their usage of OSN services, and the application of which in detecting compromised accounts. In particular, we will propose a set of social behavioral features that can effectively characterize the user social activities on OSNs. We plan to validate the efficacy of these behavioral features by collecting and analyzing real user clickstreams to an OSN website. Based on our measurement study, we will devise individual user's social behavioral profile by combining its respective behavioral feature metrics. A social behavioral profile can accurately reflect a user's OSN activity patterns. While an authentic owner conforms to the OSN account's social behavioral profile involuntarily, it is hard and costly for impostors to feign.