ON THE SECURITY OF TRUSTEE-BASED SOCIAL AUTHENTICATIONS

ABSTRACT

Recently, authenticating users with the help of their friends (i.e., trustee-based social authentication) has been shown to be a promising backup authentication mechanism. A user in this system is associated with a few trustees that were selected from the user’s friends. When the user wants to regain access to the account, the service provider sends different verification codes to the user’s trustees. The user must obtain at least k (i.e., recovery threshold) verification codes from the trustees before being directed to reset his or her password. In this paper, we provide the first systematic study about the security of trustee-based social authentications. Specifically, we first introduce a novel framework of attacks, which we call forest fire attacks. In these attacks, an attacker initially obtains a small number of compromised users, and then the attacker iteratively attacks the rest of users by exploiting trustee-based social authentications. Then, we construct a probabilistic model to formalize the threats of forest fire attacks and their costs for attackers. Moreover, we introduce various defense strategies. Finally, we apply our framework to extensively evaluate various concrete attack and defense strategies using three real-world social network datasets. Our results have strong implications for the design of more secure trustee-based social authentications.