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

Shan-Hung Wu, Man-Ju Chou, Ming-Hung Wang, Chun-Hsiung Tseng, Yuh-Jye Lee, Kuan-Ta Chen

Background

In-situ identity fraud—unauthorized, stealthy use of SNS accounts by attackers using the same device and network connection as the account owners.

The reasons that in-situ identity fraud is widespread are:

- People tend to choose "yes" when the browsers ask if they want to save their SNS passwords for automatic logins in the future.
- Mobile devices make in-situ identity fraud easy in other ways, as they can be physically accessed by acquaintances or strangers.
- SNS sites use cookies to avoid the need for account authentication within a short period of time.

We investigate the in-situ identity fraud problem in SNSs, and propose a continuous authentication approach that analyzes users' browsing behavior to detect such incidents. We show that it is possible to detect this special type of attacks on SNS sites by analyzing users' browsing behavior.

Results

There are 278 instances in our dataset which contains 178 positive and 100 negative data points with 60 features. 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.

Conclusion

- The role-driven behavioral diversity property does exist.
- The property can be exploited to design a low-cost detection scheme that is applicable to all users.
- The scheme is hard to evade and it renders a reasonable detection performance after an observation period of 2 minutes.