Abstract

Social Networking System (SNS) like Facebook and Twitter have gained more popularity in this new era. It allows millions of individuals to create online profiles and share their personal information with vast networks of friends. SNS allows third party extensions to access the users' information through Application Programming Interface (API). Since millions of users are using these sites it will lead to privacy problems and leakage of private information. This leakage happens without the knowledge of user, which leads to security problems like identity theft and phishing attack. Unknown user taking the information without our knowledge is called inference attack. This paper uses a permission based protection mechanism which limits the direct access of user data. Once an extension is certified by the user to access data from users' profile, then there is no more control on how it uses the data. Third party application can be built on trusted or un-trusted server. If it is an un-trusted server it will lead to inference attack and malicious user may use the information for unintended purposes and our data will be at risk. The main objective of this project is to enable the security access control scheme against inference attack.
References

- Chen Li, Houtan Shirani-Mehr, Xiaochun Yang (2007) "Protecting Individual Information Against Inference Attacks in Data Publishing", vol. 4443, pp. 422-433
- Facebook Newsroom. URL http://newsroom.fb.com/.
- Raymond Heathery, Murat Kantarcioğlu, and Bhavani Thuraisingham (2013) "Preventing Private Information Inference Attacks on Social Networks", IEEE Transactions on Knowledge and Data Engineering, vol. 25 pp. 1849-1862
- Zheleva E, Getoor L. "To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles.", In: Proceedings of the 18th international conference on World wide web, WWW, pp. 751e40.

Index Terms

Computer Science

Security
Keywords
Social Networking System  Application Programming Interface and Online Social Networking.