International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com || Volume 02 - Issue 06 || June 2017 || PP. 22-23

Awareness of Login Session Details through Stand alone Application

Sree Lakshmi V.
Assistant Professor, K.V.V.S. Institute of Technology,
College of MCA, Affiliated to AICTE (Under Kerala University) Adoor. Kerala – India.

Abstract: Everyone knows that today social networking sites have gained its control over the entire world. Every single human being is running after making social relationships. They feel free to share anything and everything that comes to their mind. Every moment of their life reflects now through the so called social sites. But, how much is this reliable? No one ever bothers it. How much concerned are you regarding the information you post? How much are you aware of the privacy policies? Can you assure that your personal details are not being disclosed before any third party? It has been found that every single bit of information is under the threat of exploitation by means of social network extraction methods for varying purposes. Pointing to the fact that each person's session details must be disclosed before him, so as to make him aware of his previous logins; and thereby notifying him of, any illegal or unauthorized access to his account.

Introduction

Every social networking site solely preserves the user's private account details, which are later handed over to the third parties on demand. The third parties may include the advertising companies, other social networking sites or researchers or may be legally acquired for investigation purposes. Professional hackers may also hack the details with an intension to exploitation.

Anyhow the data collected includes user id, previous history of logins and log outs, time duration of account activity, details of surfing other sites while online, purchases made if any, information searches, downloads and uploads and many more. Such collected details can be maintained as a spreadsheet and can be utilized for varying purposes.

Discussion

It is already known that disclosure of personal account details along with the session details to all users on every social networking profile is a bad choice, as it would lead to a threat to both security and privacy. Instead, what if a separate environment is set up for it?

Methods of Application

A separate application, one for each social networking site, could be designed - which when a user accepts in his personal account, provides him the details of his previous session activities, session duration etc. Clearly if a user refuses to accept the application then though the data is privately recorded by the social networking sites it will not get displayed on the user screen. Remembering the fact that hackers can exploit such applications.

Another way out is to implement a server side application. One can login to the desired social networking sites only through this explicit server side application. And all those who enter the social world through such an application could see their respective session details without fail. And those who ignore login through server application could not see the session details. But being a server machine, withholding many users, the application is under the risk of security threat.

The last and final way out is to develop a stand alone application or by other means develop a client side application. So that only those clients who run the client application and access the social network account through it, are under less risk of being hacked but still can view their session details without fail.

Result

When one comes to notice that his/her account details had been forcefully intruded without their consent and that as the session details show, the account has been in-use other than their use. They can quickly change their password as an early means of protection against exploitation.

Conclusion

The session details can be prevented by an unauthorized attack if a separate environment is being set up for it. Even if some intruders peep into your private social network accounts, the respective user will be unaware of it. As no login session details are being disclosed before them. We know that, though not all but some intruders may even exploit your personal data.

As awareness of login session details are not presently conveyed to the users, their personal data are under the risk of theft and misuse. So every social network site must show off these session details to respective users. Thereby awareness of login session details among users definitely has some impact on security breach.

Related Works

Is live visualization of your social interactions possible? Can the sites intimate or notify the live interactions on mobile phones?

Acknowledgements

For this I am grateful to the support offered to me by my colleagues and my family members.

References

[1] I. Feinerer, K. Hornik, and D. Meyer. Text mining infrastructure in R. Journal of Statistical Software, 25(5):1–54, 2008. ISSN 1548-7660. URL http: //www.jstatsoft.org/v25/i05.

[2] ISO/IEC (2005). Information technology - Security techniques - Code of practice for information security management, ISO/IEC 17799:2005(E)

[3] J. Zhao, J. Wu, and K. Xu. Weak ties: Subtle role of information diffusion in online social networks. Phys. Rev. E, 82(1):016105, Jul 2010.

[4] M. Viermetz. Partitioning Massive Graphs for Content Oriented Social Network Analysis. PhD thesis, Heinrich-Heine-Universität Düsseldorf, June 2008. URL http://docserv.uni-duesseldorfde/servlets/DerivateServlet/Derivate882 5/diss_viermetz_pdfa1b.pdf.