Online Social Network with Secure Privacy

Kartik Bhokare[1] Asif Patel[2] Sushil Ohol[3] Deepali Lokare[4]
[1,2,3,4]Department of Computer Engineering
[1,2,3,4] Zeal College of Engineering and Research, Pune, India

Abstract— The introduction of online social networks which is use to not only connect but also interact with each other as well as share information. As social network data publication is unsafe to a wide variety of re-identification and declarative attacks, developing privacy preventing mechanisms is an active research area. This paper presents a survey of the recent developments in social networks data publishing privacy risks, attacks and privacy-preventing techniques. We survey and present various types of privacy attacks and information utilized by third party user to commit privacy attacks on anonymized social network data. The survey helps readers understand the various privacy preserving mechanisms as well as observe common themes and future directions.

Key words: Social network data, Privacy attacks, Anonymized graphs, Data Privacy preserving, XSS Filter, SQL Injection

I. INTRODUCTION

Online Social Network have lead to a huge outburst of network -centric data that could be gathered for better understanding of interesting phenomena such as sociological and behavioural features of individuals or groups. As a result, online social network service operators are forced to publish the social network data for use by third party users such as researchers and advertisers.

As social network data publication is unsafe to a wide variety to re-identification and disclosure attacks, developing privacy preventing mechanisms is an active research area.

The large content of data and relationships collected by online social network operators that are quite valuable to many third party consumers.

As the social network data frequently incorporate private and sensitive information about the social network users, it is authoritative to ensure that any publish the social network data wouldn't neglect privacy of social network users.

As a result, the social network operators released sanitized version of the social network data for used by the third party users. Therefore how to preserve social network user privacy while ensuring that the published social network data is useful to the third party users is a serious challenge.

II. RELATED WORK

As shown in the previous section, publishing anonymized social graph is admitting to a significant privacy risks. In this section, we present a review of the privacy preserving approaches.

A. k-Anonymization Approach

K-anonymization model supplies anonymity through editing vertices and edges (addition / deletion) of a graph deterministically. There are three techniques used in this approach,

B. Degree Anonymization Technique:

To counter the vertex re-identification attacks the degree Anonymization approaches are designed.

These attacks done by the adversaries with prior background knowledge of the vertex degree information.

C. Neighborhood Anonymization Technique:

The neighbourhood Anonymization method is use to prevent an anonymized graph with prior knowledge of neighbourhood information from mounting the new node in graph.

D. Structure Free Anonymization Technique:

The idea is to make the vertices in the graph some like different to an adversary by making them look structurally same or similar. These anonymization approaches are designed to reduce the vertex re-identification attacks.

III. METHODOLOGY

The fundamental components of the system as shown in Figure 1 Admin module, User module, Process module, XSS filter, SQL filter etc.

In Online Social Network (OSN) there are three components

1) Admin
2) Users
3) Third Party Users

Admin which works alone on network by providing different facilities to people. Users which is nothing but the public which all are going to use this system for connection each other and last one is the third arty user who are the one of part of user also known as multiple advisers.

Process is the working system which is used to do the multiple processes like sanitization and prevention on private data.

This process is runs through XSS filter and SQL filter/injection.

The simplest and arguably the easiest form of XSS protection would be to pass all external data through a filter which will remove dangerous keywords, such as the infamous <SCRIPT> tag, JavaScript commands, CSS styles and other dangerous HTML mark-up (such as those that contain event handlers.)

The above fig shows the system architecture diagram of the system. With this system diagram it shows the how the attack will come to the system and how the attack will be affect to the system.

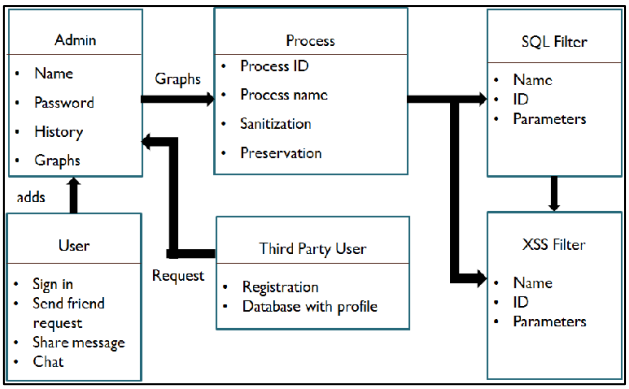

Fig. 1: Proposed Architecture

This survey Paper does an extensive study of previous developed system which tries to conclude different modules of the system using different methodologies. However the system will only be designed to recognize attacks and prevent them by using filters.

This software can be extensively used by Administrator and End-Users to provide a Social Network for communication. This Software deals with XSS. The proposed system is expected to out form existing implementation by using the anonmization techniques. The system will be designed to handle the attacks on social network.

The detection rate of XSS Detection tool can satisfy the client need, which gives the motivation to enhance the tool in the future work by adding some features covered in this thesis.

ACKNOWLEDGEMENT

The authors would like to thank all the paper and journal authors who have contributed in the field of Online Social Network privacy. The survey paper was supported under the guidance of Prof. D. Lokare. The authors are also grateful to Prof. Sunil Sangve, Head Of Computer Engineering Dept., Zeal College Of Engineering and Research, Zeal Society, Pune, Maharashtra for his valuable support.

REFERENCE

[1] Facebook. (2011). Facebook Statistic. Available: http://www.fa-cebook.com/press/info.php?statistics
[2] M. Granovetter, "The impact of social structure on economic out comes," Journal of Economic Perspectives, pp. 33−50, 2005.
[3] Y. Wang, et al., "Epidemic spreading in real networks: An ei-genvalue viewpoint," in Proceedings of 22nd International Sym-posium on Reliable Distributed Systems, 2003, pp. 25−34.
[4] N. Li and S.K. Das, "Applications of k-Anonymity and ℓ-Diver-sity in Publishing Online Social Networks, in Y. Altshuler et al. (eds.): Security and Privacy in Social Networks, Springer, pp. 153–179, 2013.
[5] P. Klerks, "The network paradigm applied to criminal organisa-tions Theoretical Nitpicking or a Relevant Doctrine for Investi-gations?," Recent Developments in the Netherlands (From Transnational Organised Crime: Perspectives on Global Secu-rity), pp. 97–113, 2003
[6] S. Ji, W. Li, M. Srivatsa, J. S. He, and R. Beyah, "Structure based Data De-anonymization of Social Networks and Mobility Traces," In S.S.M. Chow et al. (Eds): ISC 2014, Lecture Notes in Computer Science 8783, pp. 237–254, 2014.
[7] M.I.H. Ninggal and J.H. Abawajy, "Neighbourhood-Pair Attack in Social Network Data Publishing, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunica-tions Engineering, Springer-Verlag, Volume 131, pp. 726–731, 2014.
[8] W. Peng, F. Li, X. Zou, and J. Wu, "A Two-Stage De-anony-mization Attack against Anonymized Social Networks", IEEE Transactions on Computers, Volume 63, No 2, pp. 290–303, 2014.
[9] J. Williams, "Social networking applications in health care: threats to the privacy and security of health information," In Pro-ceedings of the 2010 ICSE Workshop on Software Engineering in Health Care (SEHC '10), pp. 39–49, 2010.
[10] S. Chester, B. M. Kapron, G. Srivastava, V. Srinivasan, and A. Thomo, Anonymization and De-anonymization of Social Net-work Data, Encyclopaedia of Social Network Analysis and Min-ing, pp 48–56, 2014.
[11] K. Bringmann, T. Friedrich, and A. Krohmer, "De-anonymiza-tion of Heterogeneous Random Graphs in Quasilinear Time" in A. Schulz and D. Wagner (Eds.): ESA 2014, Lecture Notes in Computer Science 8737, pp. 197–208, 2014.
[12] M. Hay, G. Miklau, D. Jensen, D. F. Towsley, and C. Li, "Re-sisting structural re-identification in anonymized social net-works. Very Large Database Journal, Volume 19, No 6, pp. 797–823, 2010.
[13] L. Backstrom, C. Dwork, and J.M. Kleinberg, "Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography," Communication of the ACM, Volume 54, No 12, pp. 133–141, 2011.
[14] X. Ying and X. Wu, "Randomizing Social Networks: a Spectrum Preserving Approach," in Proceedings of the SIAM International Conference on Data Mining (SDM 2008), pp. 739–750, 2008.

