UNIVERSITI PUTRA MALAYSIA

PRIVACY RISK METRICS AND VISUALIZATION FOR MOBILE SOCIAL NETWORKS (MSNs)

ASMAU GOGGO AHMED

FSKTM 2018 33

PRIVACY RISK METRICS AND VISUALIZATION FOR MOBILE SOCIAL NETWORKS (MSNs)

By

ASMAU GOGGO AHMED

GS46616

Supervisor: Dr Izuan Hafez Ninggal

Masters of Information Security

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

ABSTRACT

The contraption of smartphone technology has become very useful to our daily activities, most especially in terms of networking and communication, through the top five (5) most popularly used social network applications such as Facebook, Instagram, Twitter, Snapchat and LinkedIn. They create a platform where users may access, publish and share content generated by them in other to enhance their social interactions. Specifically, increased use of smartphones capable of running MSNs applications gain access to user's private information by requesting sets of permissions during installation. Hence, the lack of awareness has led to the pervasive use of background information which enable applications to be aware of a user's location and preferences.

The main objective of this dissertation is to improve MSN user's awareness on potential privacy risk after installing an application. A privacy risk metric was proposed to quantify and visualize the risk in an application. Over the years, numerous research studies have been reported on how to limit privacy leakage and improve user's awareness. However most of these studies provide relatively low privacy satisfaction and concentrated on a single pool of users.

This dissertation designs a privacy risk metrics with the use of the top 30 most dangerously requested permissions in the top five (5) MSN application, in which we categorized the various attacks on network and application in to various risk dimension by using the Confidentiality, Integrity and Availability (CIA) to quantify and visualize the total risk magnitude implication based on the permissions requested by each of the

five (5) apps after installation through a meter which makes the privacy risk interpretation easier to understand.

We conducted a survey by distributing questionnaires among Universiti Putra Malaysia (UPM) students with 147 respondents to know their level of permission comprehension when installing an application and also their preferred display style for risk visualization. However, from the results gotten we discovered that most of the users do not really understand the permission been requested by an application and so, 51.7% of the respondent choose the meter which helps in visualizing the privacy risk magnitude and also enables them to become privacy conscious.

ABSTRAK

Peranti teknologi telefon pintar menjadi sangat berguna untuk aktiviti harian kami, terutamanya dari segi rangkaian dan komunikasi, melalui lima (5) aplikasi rangkaian sosial yang paling popular seperti Facebook, Instagram, Twitter, Snapchat dan LinkedIn. Mereka membuat platform di mana pengguna boleh mengakses, menerbitkan dan berkongsi kandungan yang dihasilkan oleh mereka di lain untuk meningkatkan interaksi sosial mereka. Khususnya, peningkatan penggunaan telefon pintar yang mampu menjalankan aplikasi MSN mendapat akses kepada maklumat peribadi pengguna dengan meminta set kebenaran semasa pemasangan. Oleh itu, kekurangan kesedaran telah membawa kepada penggunaan maklumat latar belakang yang meluas yang membolehkan aplikasi menyedari lokasi dan keutamaan pengguna.

Objektif utama disertasi ini adalah untuk meningkatkan kesedaran pengguna MSN mengenai potensi risiko privasi selepas memasang aplikasi. Metrik risiko privasi dicadangkan untuk mengukur dan menggambarkan risiko dalam permohonan. Selama bertahun-tahun, banyak kajian penyelidikan telah dilaporkan mengenai bagaimana untuk membatasi kebocoran privasi dan meningkatkan kesedaran pengguna. Bagaimanapun kebanyakan kajian ini memberikan kepuasan privasi yang rendah dan tertumpu pada satu kumpulan pengguna.

Disertasi ini merekabentuk metrik risiko privasi dengan menggunakan 30 permulaan yang paling berbahaya yang diminta dalam lima (5) aplikasi MSN, di mana kita mengkategorikan pelbagai serangan ke atas rangkaian dan aplikasi ke pelbagai dimensi risiko dengan menggunakan Kerahsiaan, Integriti dan Ketersediaan (CIA)

untuk mengukur dan menggambarkan jumlah implikasi magnitud risiko berdasarkan keizinan yang diminta oleh setiap lima (5) aplikasi selepas pemasangan melalui meter yang menjadikan interpretasi risiko privasi lebih mudah difahami.

Kami menjalankan tinjauan dengan mengagihkan soal selidik di kalangan pelajar Universiti Putra Malaysia (UPM) dengan 147 responden untuk mengetahui tahap keizinan mereka ketika memasang aplikasi dan juga gaya paparan pilihan mereka untuk visualisasi risiko. Walau bagaimanapun, dari hasil yang diperolehi, kami mendapati bahawa kebanyakan pengguna tidak benar-benar memahami kebenaran yang diminta oleh aplikasi dan oleh itu, 51.7% daripada responden memilih meter yang membantu dalam menggambarkan magnitud risiko privasi dan juga membolehkan mereka menjadi privasi sedar.

ACKNOWLEGEMENTS

First of all, my deepest gratitude goes to Almighty Allah for keeping me alive and seeing me throughout the journey of discovery for my Master's Degree program.

I would like to express my sincere gratitude, thank my delightful supervisor Dr. Izuan Hafez Ninggal for his unwavering enthusiasm, guidance and immense support which kept me constantly engaged with my research.

My appreciation goes to all academic staff and my fellow course mate of Department of Information Security for their personal generosity, helped made my time at Universiti Putra Malaysia (UPM) enjoyable and my lovely parents for their sponsorship of this Master Degree.

I would also like to thank Bokolo Anthony and Abubakar-sadiq Mohammed for much excellent advice and all sort of issues and for reading a draft of the thesis; and Also Prof Nor Fazlida Binti Mohd Sani for her genuine kindness which also helped sustain a positive atmosphere in carrying out this project research.

Above all ground, am indebted to my family, whose value to me only grows with age. And finally I acknowledge my mum, Engr. Mrs. Mariam Ahmed who is my champion and who blessed me with a life of joy in times when I was down.

DEDICATION

My humble effort is dedicated to my sweet and loving **MOTHER AND FATHER** Whose affection, love, encouragement and their daily prayers made me achieve such a great success. Alongside all the hardworking and respected lectures of Department of Information Security **FSKTM.**

DECLARATION

I hereby declare that the thesis is based on my original work except for quotations and citation which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UPM or any other institution.

ASMAU GOGGO AHMED

Date: 23 January 2018.

APPROVAL SHEET

This thesis is submitted to the Faculty of Computer Science and Information Technology of University Putra Malaysia and has been accepted as partial fulfilment of the requirements for the Masters of Information Security.

Dr. Izuan Hafez Ninggal

Department of Information Security

Faculty of Computer Science and Information Technology,

UniversitI Putra Malaysia.

Date: _____

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
API	Application Programming Interface
EFA	Exploratory Factor Analysis
GPS	Global Positioning System
LS	Location Service
LSB	Location Service Base
LPPMs	Location-Privacy Protection Mechanisms
MSN	Mobile Social Network
MSNs	Mobile Social Networks
MNSP	Mobile Network Service Provider
PRM	Privacy Risk Metric
P2P	Peer-to-Peer
RAM	Random Access Memory
SDK	Software Development Kit
SNA	Social Network Application
SPSS	Statistical Package for Social Science
TTP	Trusted Third Party
UPM	Universiti Putra Malaysia

CHAPTER 1

INTRODUCTION

1.1 Overview

The use of Mobile Social Networks (MSNs), has become a major stipulation worldwide. Through the use of MSNs, users may access, publish and share content generated by them at anytime and anywhere, enhancing their social interactions. MSN applications are characterized by the integration of background information to the social network content, enriching the existing applications and providing new services. Due to the prevalence of (MSNs) the jeopardy of privacy proliferating breaches has increased as a result of location disclosure by end users.

On the contrary, the lack of awareness and the pervasive use of background information leads to new privacy and security challenges, which is the scope of this proposal, which aims to describe the main concepts, research challenges and solutions for this area. Conversely, mobile social networks (MSNs) such as Facebook check-Ins, Weibo, or Renren fascinate lots of users by employing point of enthusiasm acquirers, friend discoverers, geosocial networking, etc.(Li, Zhu, Du, Liang, & Shen, 2016) Consistently, these mobile social networks (MSNs) operates as clienteles to location services such as Google Latitude or Yahoo Fire Eagle, and that aids in admonishing mobile object in MSNs and assures scalability to assist innumerable clients with mobile object positions.

However, when trying to calibrate the location privacy leakage from MSNs there is a need in coordinating the users 'communal locations with their real mobility traces by so doing, the users definite location is being disclosed which hikes the need for an extensive disquiet of the user's privacy specifically, if location service providers are not copiously credible, and this may lead to the leakage, adrift and embezzlement of private position information.

In MSNs, numerous conceptions and methodologies for location privacy protection have been designated in the collected works. These methodologies are variance with respect to the secured information and their efficiency alongside different attacks (Wernke, Durr, & Rothermel, 2012). A survey was carried out in order to know, how aware are the MSN users in terms of permission granting when downloading an application. Somewhat it turned out that the survey was only carried out on only computer science students, which was one limitation of the research (Lopez & Wu, 2015). Although, (Ardagna, Cremonini, De Capitani Di Vimercati, & Samarati, 2011) operators, that, when used individually or in combination, protect the privacy of the location information of users. However, the work presented by, (Ardagna et al., 2011) leaves space for further works.

Quantification and visualization of location privacy risks in MSNs has been a prime area of research since the last few decades, and this space of study has received vastly an awesome response and contribution from researchers. Quantification and visualization for privacy risks is one of the core actions in IT governance. However, quantification and visualization can be defined as progression for ascertaining risk and

deciding the most suitable approach in moderating the risk according to the intents of it experts which includes classifying, analysing and evaluating possible attacks through the proposed models. This models tends to give MSN users a clearer understanding about the risk involved with location sharing applications in MSNs. The quantification and visualization of privacy risks provides a mechanism for MSN users to be aware of the kind of risk they are dealing with in an application while using the MSN, thus presenting a medium to understand and express the visualization study of location privacy in MSNs for users (Lopez & Wu, 2015).

Quantifying and visualizing privacy risk can be said to be an essential process to assist MSN users, by enabling users to continuously sense and visualize the risk in sharing their locations and social context via mobile social apps, and receive accurate and high-quality location-based and personalized service. However, this tends to improve the awareness of MSN users when using several location sharing applications.

1.2 Problem Background

The central delinquencies currently with MSN users, has to do with the evolving of mobile devices from simple phones to sophisticated computing systems, the data stored on these multi-tasking device have subsequently come to be more sensitive and private. Due to this, advancement of mobile operating systems which consist of new agreement systems for confining the access to the device for MSNs. Nonetheless, numerous MSNs acquire more permissions than required. These over-privileged applications can affect data security and user location privacy. All application permissions are indicated to the user, but these notifications have been shown to be

ignored or not understood. Thus, other mechanisms can be improved by moderating the probability of various MSN's in which users can have an awareness of applications they are involved with.

1.2.1 Privacy Warnings Messages are hard to Interpret by Users on Permissions (Requesting to Access Location)

Privacy warnings are very essential in applications most especially MSN's. Although majorities of MSN applications have privacy terms which most users find it very difficult to interpret. MSN user's state of mind about permission granting and privacy are quite intricate and often inconsistent. Due to the absence of understanding. Survey carried out by previous researcher has shown that, most MSN users are so protective about their location. However, most MSN user's engagements do not always relate to their supposed preferences (Ruiz Vicente, Freni, Bettini, & Jensen, 2011). This may be because MSN users tend to overestimate their privacy and also as a result of minimal understanding of the permission request they are granting to the so called service providers.

1.2.2 Users Do Not Pay Attention to Permission Warnings

Most of the time when a user tries to installs an MSN location application from Google play (the official market place for acquiring apps in Android), users are mostly asked sets of permissions for apps to access location information or use features from their smartphones. Nonetheless, reviews (Lin et al., 2013) have publicized that majority of MSN users ignore and at the same time do not pay attention to permission warnings. Since debate and apprehension are fundamentals for conversant security and privacy

verdicts. For instance (Felt et al., 2012) revealed in their survey, that 83% of android users who took part in their study did not really pay attention to permission notification screens, only 3% of users properly inferred the meaning of permission granting. Although scheming an operational warning message system form permission appears absolutely perplexing, [6] there is a need for privacy facts in order to give efficient warning display about permissions.

1.3 Research Questions

1. How to improve MSN user's awareness of potential privacy implications on permissions and location privacy risk after installing an application.
2. How to create a metrics in quantify the privacy risk in MSN?
3. How to make users pay attention through visualizing the privacy risks in applications.

1.4 Research Objectives

The objectives of this study are as follows:

1. To improve MSN user's awareness of potential privacy implications on permissions and location privacy risk after installing an application.
   (i) To propose a metrics in quantifying privacy risks to enable users have clearer understanding.
   (ii) To visualize location privacy risks based on the quantification to enable users pay attention to permission warnings.

1.5 Research Scope

This thesis covers a quantification and visualization of location privacy risks in MSNs. The scope of this thesis is encompassed below:

As location services presently attracts heaps of mobile users. Although, with the popularity of these services, their usage has raised severe privacy concern as most users are unaware of the privacy risks involved with MSNs. For example, most Mobile Network Service Providers (MNSP) reveal a user's actual location which may grant an attacker to glean receptive information if a user visits, for instance, a hospital or bank. (Wernke et al., 2012). Conversely, our research will focus on quantifying and visualizing location privacy risks for MSNs will only focus on permission granting and awareness on location services provided by numerous Mobile Network Service Providers (MNSP). Likewise, the divulged of a user data could be exploited for stalking and assaulting. According to [3]. Most MSNs user are not aware of the implication of neglecting permission warning, sharing their location and granting access. Therefore it is important to quantify and visualize the privacy risk for better awareness for location privacy in MSNs.

A specific research type was adopted, in our research we used a case study to find out MSN users level of understanding of permission request displays, awareness and privacy conscious among MSN users from different countries, faculties and age groups in Universiti Putra Malaysia. In the case study, data is collected using questionnaires from 149 respondents. Based on the case study technique stated by [2].

[3]. the minimum number of informant in the case studies was 36 and the maximum was 308. Although the number of informants can be more than or below 308.

1.6 Research Contribution

The contribution of this thesis is to design a meter which will quantify and visualize the location privacy risk in MSN's. In this way the research contribution of this thesis is elucidated as follows:

1) Privacy Quantification Metrics

This research identifies the process and components involved in quantifying the privacy risks through a Privacy Risk Metrics (PRM) in MSNs. MSN users will use the identified process of location privacy risk quantification components as a guideline in making decisions on whether a particular application has more or less risk in terms of number of permissions requested and location analysis.

2) Risk Visualization

This research designed a meter which comprises of a quantified risk metrics and visualizes the process using a slider bar. The components of the privacy meter signifies if the risk is LOW, MEDIUM and HIGH using colours and also has a privacy awareness agents which helps in informing users on possible attacks as well as the location analysis. The model shows how location privacy risk is being quantified and visualized in mobile social networks (MSNs). Additionally location privacy risk quantification and visualization metrics is developed to implement the location privacy meter which enlightens MSN users pertaining to the location privacy risk

awareness and decisions after installing a social network application such as Facebook, twitter etc.

3) Survey Outcome

While trying to design a metric in visualizing the privacy risk in MSN, an online survey was carried out having a total of 147 respondents. The survey was conducted amongst Universiti Putra Malaysia students to be able to know their level of permission comprehension and privacy consciousness. Hence, results gotten from the survey to some extent influenced the aforementioned contributions.

1.7 Summary

This chapter summaries the whole concept concerning privacy risk in mobile social networks. However, the chapter gives a brief introduction about MSNs, permission comprehension, location privacy as well as challenges that MSN user's encounter. Without further a dew, the chapter also discusses on the problems, scope and objective of our proposed privacy metrics in quantifying and visualizing privacy risk in MSNs.

1.8 Dissertation Organization

The rest of the dissertation is organized as follows:

Chapter 1 introduces the research area of concern. The chapter begins with a portrayal of the research background, encompassing the focus of previous research relating privacy risk, problems arising based on previous studies. The chapter proceeds with a problem statement, containing the identified problems from previous studies. The

chapter then clearly describes the research objectives, research questions and the scope of the research.

Chapter 2 presents an overview of a comprehensive review which lays a conjectural explanation on location privacy attacks as well previous research works that addressed issues related to permissions comprehension and location privacy risks in MSNs.

Chapter 3 explores the research methodology and explains the phases in details. The proposed metrics for quantifying and visualizing privacy risks are also presented in this chapter.

Chapter 4 describes the results and discussion based on the feedback from our online survey in trying to know the level of awareness it terms of privacy consciousness and permission comprehension by MSN users. We had a total of 147 respondent within Universiti Putra Malaysia (UPM) campus.

Chapter 5 presents the design which discusses the privacy leakage framework and architecture of the proposed Privacy Meter. It describes the metrics and presents the performance evaluation for visualizing the privacy risk in mobile social network as well as the location analysis.

Chapter 6 concludes the dissertation by describing the research outcomes in relation to the achievement of the research question, research problem and research objectives. The chapter then summarizes the work and recommends some promising directions for further research to be done.

REFERENCES

Ardagna, C. A., Cremonini, M., De Capitani Di Vimercati, S., & Samarati, P. (2011). An obfuscation-based approach for protecting location privacy. *IEEE Transactions on Dependable and Secure Computing*, *8*(1), 13–27. https://doi.org/10.1109/TDSC.2009.25

Bigwood, G., Abdesslem, F., & Henderson, T. (2012). Predicting Location-Sharing Privacy Preferences in Social Network Applications. *Proceedings of the First Workshop on Recent Advances in Behavior Prediction and pro-Active Pervasive Computing (AwareCast) (June 2012)*, 1–12. Retrieved from http://www.ibr.cs.tu-bs.de/dus-beigl/Awarecast/awarecast2012_submission_1.pdf

Chow, C. Y., Mokbel, M. F., & Liu, X. (2011). Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments. *GeoInformatica*, *15*(2), 351–380. https://doi.org/10.1007/s10707-009-0099-y

Damiani, M. L. (n.d.). Location privacy models in mobile applications: conceptual view and researc...: EBSCOhost. Retrieved from http://web.b.ebscohost.com.tcsedsystem.idm.oclc.org/ehost/pdfviewer/pdfviewer?vid=1&sid=6bf91c12-fe1e-4e11-a92f-ffcc645d2dc8%40sessionmgr101

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android Permissions: User Attention, Comprehension, and Behavior. Retrieved from https://cs.umd.edu/class/spring2017/cmsc818O/papers/android-permissions-attention.pdf

Li, H., Zhu, H., Du, S., Liang, X., & Shen, X. (2016). Privacy Leakage of Location Sharing in Mobile Social Networks: Attacks and Defense. *IEEE Transactions on Dependable and Secure Computing*, *5971*(c), 1–1. https://doi.org/10.1109/TDSC.2016.2604383

Lin, J., Benisch, M., Sadeh, N., Niu, J., Hong, J., Lu, B., & Guo, S. (2013). A comparative study of location-sharing privacy preferences in the United States and China. *Personal and Ubiquitous Computing*, *17*(4), 697–711. https://doi.org/10.1007/s00779-012-0610-6

Lopez, J., & Wu, Y. (2015). Information security practice and experience: 11th International Conference, ISPEC 2015 Beijing, China, May 5–8, 2015 proceedings. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9065*, 548–558. https://doi.org/10.1007/978-3-319-17533-1

Meissner, H., Creswell, J., Klassen, A. C., Plano, V., & Smith, K. C. (2011). Best Practices for Mixed Methods Research in the Health Sciences. *Methods*, *29*, 1–39. https://doi.org/10.1002/cdq.12009.

Ruiz Vicente, C., Freni, D., Bettini, C., & Jensen, C. S. (2011). Location-related privacy in Geo-social networks. *IEEE Internet Computing*, *15*(3). https://doi.org/10.1109/MIC.2011.29

Vidas, T., Christin, N., & Cranor, L. F. (2011). Curbing Android Permission Creep. *IEEE Web 2.0 Security and Privacy Workshop (W2SP)*.

Wei, W., Xu, F., & Li, Q. (2012). MobiShare: Flexible privacy-preserving location sharing in mobile online social networks. *Proceedings - IEEE INFOCOM*, 2616–2620. https://doi.org/10.1109/INFCOM.2012.6195664

Wernke, M., Durr, F., & Rothermel, K. (2012). PShare: Position sharing for location privacy based on multi-secret sharing. *2012 IEEE International Conference on Pervasive Computing and Communications, PerCom 2012*, (March), 153–161. https://doi.org/10.1109/PerCom.2012.6199862

Wernke, M., Skvortsov, P., Dürr, F., & Rothermel, K. (2014). A classification of location privacy attacks and approaches. *Personal and Ubiquitous Computing*, *18*(1), 163–175. https://doi.org/10.1007/s00779-012-0633-z

Ding, Y., Peddinti, S. T., & Ross, K. W. (2014, November). Stalking beijing from timbuktu: a generic measurement approach for exploiting location-based social discovery. In *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices* (pp. 75-80). ACM.

Li, M., Zhu, H., Gao, Z., Chen, S., Yu, L., Hu, S., & Ren, K. (2014, August). All your location are belong to us: Breaking mobile social networks for automated user location tracking. In *Proceedings of the 15th ACM international symposium on Mobile ad hoc networking and computing* (pp. 43-52). ACM.

Polakis, I., Argyros, G., Petsios, T., Sivakorn, S., & Keromytis, A. D. (2015, October). Where's Wally?: Precise user discovery attacks in location proximity services. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 817-828). ACM.

Ardagna, C. A., Cremonini, M., di Vimercati, S. D. C., & Samarati, P. (2011). An obfuscation-based approach for protecting location privacy. *IEEE Transactions on Dependable and Secure Computing*, *8*(1), 13-27..

Pasick, R. J., Burke, N. J., Barker, J. C., Joseph, G., Bird, J. A., Otero-Sabogal, R., ... & Washington, P. K. (2009). Behavioral theory in a diverse society: Like a compass on Mars. *Health Education & Behavior*, *36*(5_suppl), 11S-35S..

Erhard Rahm., Hong Hai Do “Data cleaning problem and current approaches” University of Leipzig, Germany http://dbs.uni-leipzig.de 2010

Shokri, R., Theodorakopoulos, G., Le Boudec, J. Y., & Hubaux, J. P. (2011, May). Quantifying location privacy. In *Security and privacy (sp), 2011 ieee symposium on* (pp. 247-262). IEEE.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (1998). *Multivariate data analysis* (Vol. 5, No. 3, pp. 207-219). Upper Saddle River, NJ: Prentice hall..

Helms, J. E., Henze, K. T., Sass, T. L., & Mifsud, V. A. (2006). Treating Cronbach's alpha reliability coefficients as data in counseling research. *The Counseling Psychologist*, *34*(5), 630-660.

Cooper and Schindler 2008. Surveys in Social Research. (5th Ed.) Australia: Crows Nest, NSW.

Curwin, J. and Slater, R. 1991, Qualitative Methods for Business Decisions. London: Chapman and Hall

Creswell, J. (2009). Research Design: Qualitative, quantitative, and mixed methods approaches, Los Angeles, SGE Publications, Inc.

Kumar, R. (2005). Research methodology: A step-by-step guide for beginners. Sage. *https://www.slideshare.net/MuhammadIbrahim15/data-analysis-using-spss*

Becher et al., 2011; Enck et al., 2011; Hogben and Deker, 2010; Jansen and Ayers, 2007; Jeon et al., 2011; Lederm and Clarke, 2011; OWASP, 2013; Shabtai et al, 2010).

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012, July). Measuring user confidence in smartphone security and privacy. In *Proceedings of the eighth symposium on usable privacy and security* (p. 1). ACM.

ISO. Information technology Security techniques - Information security risk management. Technical Report ISO/IEC 27005:2008.