2012 International Conference on Networks and Information (ICNI 2012)

IPCSIT vol. 57 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V57.22

The Analysis of Social Network Factors Toward Social Engineering Attack :Case Study on Facebook.com using in Thailand

Pagon Gatchaee [+]

School of Computer Science and Engineering, Beihang University, Beijing, China

Abstract. Social network is very important and a lot of effective to user who surfing internet in cyber world because social network help people to communicate together and very easy to make friend even never know in real world. So attacker use social network activity and user behavior in social network as medium and tools for attack by social engineering technique due to social engineering technique is attacking technique that regard to human behavior.
From above, researcher analyzed to get social network factors toward social engineering attack by using survey with sample group of facebook.com's users in Thailand.

Keywords : Social engineering, Social network, social network analysis

1. Introduction

This research used questionnaire to survey people in Thailand who use Facebook.com that famous social network in present. For questionnaire, there are questions about social network activities and social engineer attack tricks that analyzed from many related research papers [1],[2],[3],[4],[5] to use as question in questionnaire.

2. Surveying a sample group in Thailand

From review many research papers in a field of social network security with make a survey from 120 facebook users in Thailand (http://www.surveycan.com/survey101581) that can described about this survey as followings:

2.1. Sample group in Thailand

According to Internet World Stats, Thailand is ranked 9th in 2011 amongst countries in Asia [7] and the top reason for using the internet among teenagers aged 14-19 is social networking that can see a significant increase in the number of people who uses social networking services as fig 1.

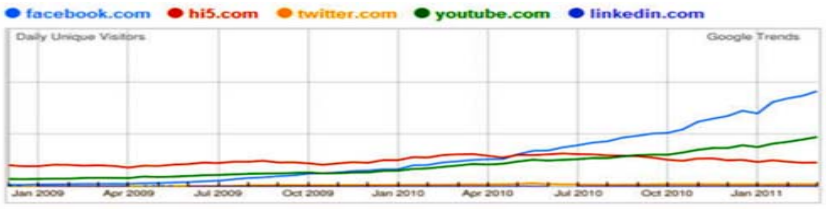

Fig1. Increase in users for various social networkng service in Thailand since Jan 2009 – Jan 2011 [9]

For most popular social network in Thailand , That site is "Facebook.com" which is the number one most popular user-gernerated content website and the most used social networks as of 25 May 2010 in

[+] Pagon Gatchaee. Tel.: +(86-1881-051-4952*). E-mail address*: (ploiro@gmail.com)

Thailand [9] .Currently, there are 14 Million Facebook users in the Thailand, which makes it no.16 in the ranking of all Facebook statistics by country.

From above descriptions ,we will know social network especially Facebook.com is very impact to Thai people so should to analyze and collect information about social network activity and behavior for use in this research from Thai people.

2.2. Survey factors

In this survey will have many survey factors that should be regarded as

3.2.1 Confidence level

For this survey , will use confidence level as 95% for make sure that user can trust result from this survey .

3.2.2 Sample size

Since 1 April – 16 April 2012 ,author can collect data from 213 participants who answer this survey .

3.2.3 Population

This survey , will use population as total of Thai facebook users .It approx 14,000,000.

3.2.4 Calculate confidence level for evaluate trustable of survey

$$ss = \frac{Z^2 * (p) * (1-p)}{c^2}$$

Where: Z = Z value (e.g. 1.96 for 95% confidence level) ,p = percentage picking a choice, expressed as decimal (.5 used for sample size needed) ,c = confidence interval, expressed as decimal (e.g., .04 = ±4)

From above formula which formula to calculate sample space but now we already had sample space as 213 so we can use this formula to calculate confidence level that have a result is 6.71.

Finally , we got confidence level as 6.71 which can denoted to result of this survey quite can trusted due to confidence interval not too much although actually should be 5 if use confidence level as 95% but 6.71 still in acceptance confidence interval period.

2.3. Purpose of survey

From 3.1 , we will get description about Facebook activity , behavior , demography (age , sex) so result from this survey have to regard and consistent with 3.1 .

In addition ,question and result from this survey have to able to analyze factor toward social engineering attack .

3. Social network factors toward social engineering attack

From survey in section 3., found social network factors toward social engineering attack as

3.1. Privacy issue

Privacy issue is most importance factor that toward social engineering attack because privacy issue made from user and will regard and effect to user in social network

For privacy factor , user have to realize on private data such as biography information, Photo, Shared link, Posting content both from profile owner and friends, Tagging data from friends and others in social network site.

From survey, researcher found user not set a privacy security into private status or can access only friend or anybody who trustable .Many user always retain a public status and always share private data without consider privacy security.

3.2. 3rd party social network service

In nowadays, There are many 3rd party social network service that will connected together with main social network service .In study case of Facebook , There are many 3rd party service as mobile social network service (Instagram ,Path ,Lightbox ,etc.) and other social network site as twitter , youtube ,msn ,skype.

From fig2 (Pink color is none of using 3rd party) ,author found many people will use 3rd party with main social network site and allow 3rd party can post data and get data from main site that bring to difficult control private and privacy security and toward to social network attack .

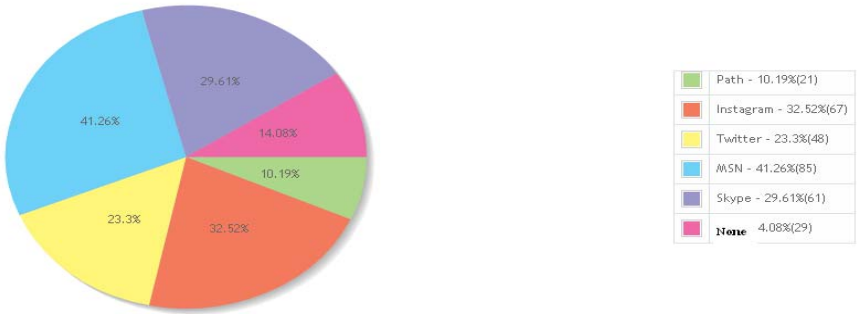

Fig2. Circle graph to display 3rd party used in facebook percentage

3.3. Geo Social network issue

Geo Social network issue is a issue from social network service that allow people share and post geo-location into social network such as check-in service 3rd party such as Path,FourSquare that mentioned in 4.2 that attacker can analyze and get location for attack user both for online and offline attacking .

Moreover, due to new image technology as EXIF format that currently embed into new mobile and camera device such as iPhone which a famous smart phone in present that embedded geo location (Latitude, Longitude) .So, attacker can extract this information from user photo which post in social network for a moment time and then attack user both for online and offline as same as geo social network service that already mentioned it as above.

From fig3, found many people never know about EXIF format (Green is know, Orange is none of knowledge) that will be victim by attacker.

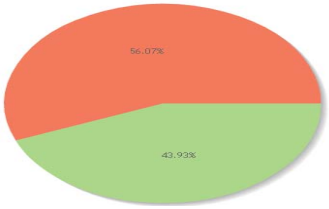

Fig3. Circle graph to display percentage between user who know and none of knowledge about EXIF

3.4. Frequency of social network using

From survey, found one of social engineering attack as tagging in photo or post as spam depend on frequency that mean when user accessed facebook by more frequency than others, that user may be victim by possibility than others.

From fig 4, found most user who access facebook everyday are tagged in photo or post as spam than others (tagged and can remove -Green, tagged and cannot remove -Orange, tagged and do not know how to remove-Yellow, never tagged-Blue).

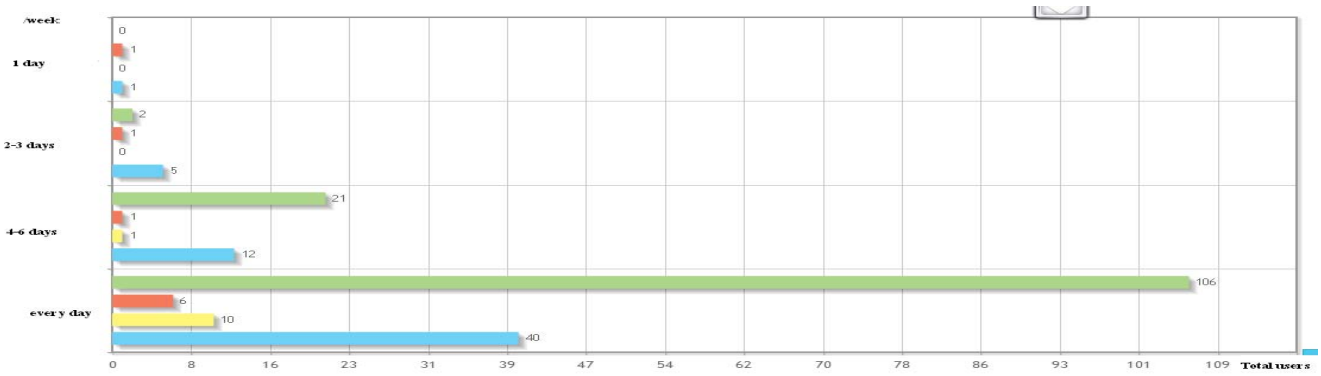

Fig 4. Bar chart to display frequency of facebook using per week with tagged in photo or post as spam

4. Conclusion

This research analyzes and presents social network factors that toward to social engineering attack by research from research paper and use a survey from facebook's users in Thailand as sample group.

5. Acknowledgements

Thank you Prof.Zhoujun Li, The professor of School of Computer Science, Beihang University as supervisor.

6. References

[1] "Using Facebook to Social Engineer Your Way Around Security", http://www.eweek.com/c/a/Security/Social-Engineering-Your-Way-Around-Security-With-Facebook-277803/ 05.20.2010.

[2] B. Zhou and J. Pei, "Preserving Privacy in Social Networks Against Neighborhood Attacks", IEEE International Conference on Data Engineering (ICDE),2008

[3] M. Huber, "Automated social engineering, proof of concept," Master's thesis, DSV SecLab, Stockholm University/Royal Institute of Technology, Mar. 2009. [Online]. Available: http://asebot.nysos.net

[4] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks (the Facebook case)," in Proceedings of the 2005 ACM workshop on Privacy in the electronic society, 2005, pp. 71–80.

[5] S. B. Barnes: A privacy paradox: Social networks in the United States. http://www.firstmonday.org/issues/issue11 9/barnes/index.html. Retrieved 29 Oct 2008

[6] "Social Engineering (security)" , http://en.wikipedia.org/wiki/Social_engineering_(security). Retrieved 10 April 2012.

[7] Thailand's Internet User Population , http://www.internetworldstats.com/stats3.htm. Retrieved 15 April 2012.

[8] Bangkok has most Facebook users in world , http://www.thephuketnews.com/bangkok-has-most-facebook-users-in-world-30721.php. Retrieved 19 May 2012.

[9] Digital media in Thailand , https://wiki.smu.edu.sg/digitalmediaasia/Digital_Media_in_Thailand. Retrieved 15 April, 2012.

Pagon Gatchalee He was born in Bangkok, Thailand. He is Master degree candidate on Computer software and Theory at Beihang University Beijing, China. His interesting research fields are social network, web technology and its applications, information security and software development method.