International Journal of Electrical and Computer Engineering (IJECE)
Vol. 5, No. 2, April 2015, pp. 175~176
ISSN: 2088-8708

Editorial

Social Network Applications and Free Online Mobile Numbers: Real Risk

Mehdi Dadkhah*[1], Tole Sutikno[2], Shahaboddin Shamshirband[3]
[1]Young Researchers and Elite Club, Tiran Branch, Islamic Azad University, Tiran, Iran
[2]Department of Electrical Engineering, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[3]Department of Computer System and Information Technology, Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia
*Corresponding author; e-mail: dadkhah80@gmail.com[1], tole@ee.uad.ac.id[2]

Social network applications are being more widely used among users and new types of such applications are created by developers. Almost all users who use smart phones are users of such application [1]. Major concern in these applications is privacy and security [2]. We can name WhatsApp, Viber, Facebook, Telegram, Line, WeChat and Beetalk as the most popular applications. There are also websites which provide online numbers in order to receive SMS. The goal of this website is providing anonymous virtual phone number to protect users from spam. Also these sites provide different number from different countries and let people to can use them for different application. The services of these websites are divided into two groups: subscription services in which a unique number is assigned to the user by charging him/her and free services in which user can see the received messages of some online numbers without any registration. Table 1 shows examples of these websites.

Table 1. Free online numbers from different country

Website URL	Country availability in free service	Average Visitor per day
http://receivesmsonline.com	Canada, Finland, Germany, United Kingdom, Sweden, Poland	4460
http://www.receivesmsonline.net	Canada, Germany, United Kingdom, Sweden,	4420
http://receive-sms-online.com	Norway, Poland, Ukraine, Germany	5000
http://receive-sms-now.com	Canada, Finland, Germany , Sweden, Poland, Mexico, Belgium, Hong Kong	4100
http://hs3x.com	Canada, Germany, United Kingdom, Sweden, USA	4140

Most communication and social network applications of smart phone use users' cell phone numbers for authentication; they ask user to enter his or her cell phone number while installing the application; and after he or she enters the phone number an SMS containing an activation code is sent to user from the application server. The user can use the social network application after entering the code and the default number of the application is set the phone number which the user enters during activating the application. In other word these application use phone number for authentication and any people access to phone number can see all information and personal data.

Many users use websites providing free numbers for receiving SMS in order to enter their numbers in their social network applications. After installing the social network application, the user enters one of the numbers existing in SMS receiving provider websites instead of his/her own phone number and activates the application. The main problem of this activation method is that it is possible several users use a free number for activating the application. Therefore, they can access messages sent to each other and one of the basic principles of security [3], i.e. confidentiality is violated. For example we visited a free SMS receiving provider websites and observed that the Line application has been activated by the same number for 154 times. Figure 1 shows website that provide free online number (http://receivesmsonline.com) with different social network application that registered by its numbers in one day.

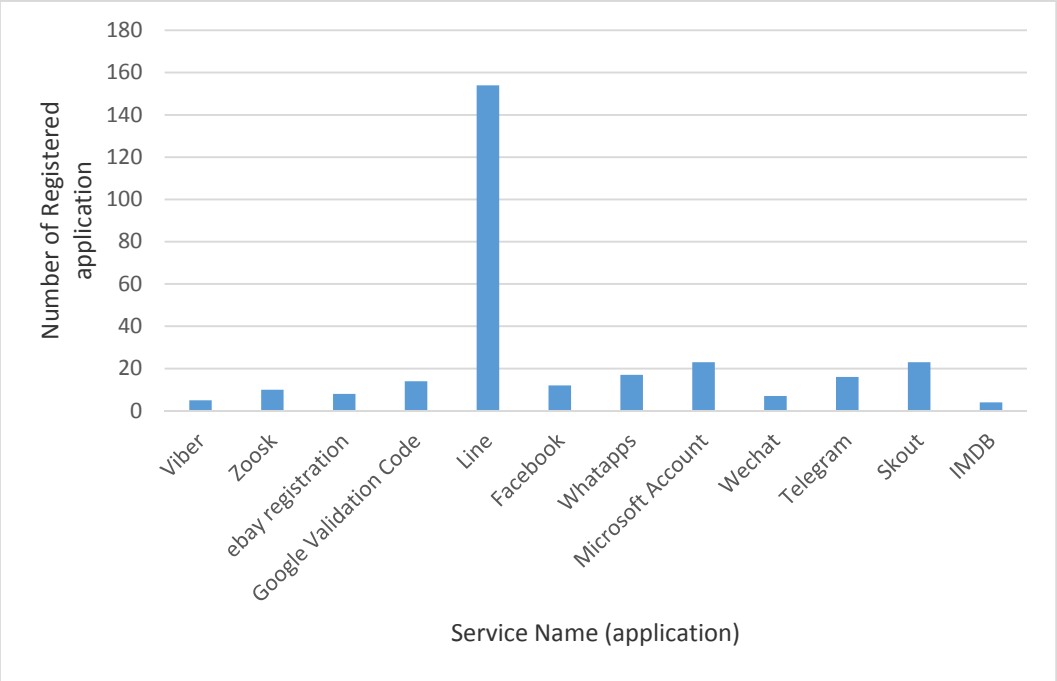

Figure 1. Number of registered application by free online number website in one day.

In addition, some applications such as Telegram store user information like previous messages and personal picture in their server. When another application is activated by the same free number, all their private information is accessible for the second person. In some case attacker can change user's password and gain access to their information. For example if user used free online number for his/her Facebook account, attackers can restore his/her password. Table 2 shows vulnerable application to free online mobile numbers. These application use SMS authentication that can be exploit by attackers, in case that application used call authentication it is not possible to exploit by attackers.

Table 2. Vulnerable application to free online mobile numbers.

Application or service name	Vulnerable	Description
Viber	Yes	Allow user to register different applications with same number I windows version
Line	Yes	Allow user to register different applications with same number
Whatapps	Yes	Allow user to register different applications with same number
Wechat	Yes	Allow user to register different applications with same number
Telegram	Yes	Allow user to register different applications with same number
Facebook	Yes	It I possible that attacker restore password by using free number
Beetalk	Yes	Allow user to register different applications with same number

So the SMS receiving provider websites should not be used for activating communication applications. On the other hand, the developers of these applications should find a solution for this major weakness and don't allow activating several similar applications by the same number.

References

[1] Zin T, Tin T, Hama H, Toriu T. *Knowledge based Social Network Applications to Disaster Event Analysis*. Proceedings of the International MultiConference of Engineers and Computer Scientists. Hong Kong. 2013: 1-6.
[2] Chin E, Fel A. P, Sekar V, Wagner D. *Measuring User Confidence in Smartphone Security and Privacy*. Proceedings of the Eighth Symposium on Usable Privacy and Security. Washington. 2012; 1-16.
[3] Prasad P, Ojha B, Shahi R. R, Lal R. *3 Dimensional Security in Cloud Computing.* 3rd International Conference on Computer Research and Development (ICCRD). Shanghai. 2011; 3: 198-201.