International Journal of Academic Engineering Research (IJAER)
ISSN: 2643-9085
Vol. 3 Issue 12, December – 2019, Pages: 8-12

# Considerations on Confidentiality in Social Networks Using Two-Factor Authentication

**[1]Nzisabira Louis and [2]Abubakarsidiq Makame Rajab**
[1]M&N Solutions 42, Revolution Street, P.O.Box: 1342, Bujumbura, Burundi.
[2]School of Electronic Information Communication, Huazhong University of Science and Technology,
Hongshan District, Wuhan 430074, P.R. China
[1]**Email:**louisnzisabira@outlook.fr **and** [2]**Email:** mrgovery@hotmail.com

***Abstract***— *The study point out an evaluation in Network and Information Security course. It's a Survey on Security Issues in Social Networks. Use of Social Networks goes increasing. A huge amount of information they contain makes them and users on them privileged target of diverse attacks and threats. Network and Information Security is a major part of IT and professional in related domains have carried many researches about it. Different principles, concepts, mechanisms, methods, techniques and other aspects have been implemented to ensure and strengthen security on devices, data, networks, and clouds and so on. Advantages and challenges occur at different levels. Among other different methods applied on different accounts in social networks as well as in emails, one is using phone as a supplement factor way of authentication. The survey discusses some considerations on confidentiality in Social Networks, name breaches and threats, and especially the two-factor authentication using mobile phone, its advantages and challenges. At the end we present our conclusion and give an idea on possible further research as a way to strengthen confidentiality and avoid regrets in social networks.*

**Keywords**— Network and Information Security, Social Networks, Two-Factor Authentication.

## I. INTRODUCTION

Since some years especially the last decade, social networks are increasingly gaining in number of users all over the world. They cover a wide range of web and internet based applications and services that allows individuals to construct a public or semi- public profile within a bounded system. The fact is that social networking often involves grouping specific individuals or organizations together. And in add, by persistent information users leave or post on social networks about themselves or their friends. It's another way of identifying and giving a huge amount of data possible to be re-exploited in other ways and others actors initially not involved in. Social networks are structured or personal networks, with individual at the center of their own community [1].

Some of social networks include also collaborative tools such as the personal profile and friendly links which are commonly supported by commercial. On registration, some social networks sometimes require sensitive information. Some range from almost complete identity by filling or completing forms that record the date and place of birth, the gender, the field of activity. For extensive use, some social networks such as WeChat request information on the portfolio of their users, such as the bank account number to allow financial transactions. Social networks also allow and incite almost to expose of his academic, professional and family life. With such multiple and various interconnection of social networks and others interested services, security issues and protection of private information online has been a serious and important research topic. Our survey tries to explore and discusses some considerations on confidentiality in Social Networks, name breaches and threats, and especially the two-factor authentication using mobile phone, its advantages and challenges. At the end we present our conclusion and give an idea on possible further research as a way to strengthen confidentiality and avoid regrets in social networks [2].

## II. INFORMATION SECURITY AND PRINCIPLES

Information Security, definition and main principles, it is a general expression that can be used regardless of the form the data may take whether electronic or material. In one hand security management concepts and principles are inherent elements in a security policy and solution deployment. They define basic parameters we need for a secure environment. In the other hand they are objectives and goals to be achieved in regard of obtaining a secure solution. The triad confidentiality, integrity and availability are the commonly accepted foundation of secure information and environment in which it's processed. Security controls are typically evaluated on how they address these core information security tenets.

First, Confidentiality ensures that high level of assurance that data, objects, resources, processes involved in standalone environment, in a system, networks or cloud and other possible means involved in are restricted from unauthorized subjects. The second principle of the CIA is integrity. This means that data or objects must retain their veracity and be intentionally modified by only authorized subjects. It involves the maintenance of internal and external consistency of objects so that their data is a correct and true reflection of the real world and all relationship are valid, consistent, and verifiable. Confidentiality and integrity are closely interdependent on each other. No integrity without confidentiality. Breaking confidentiality allows to breaches in integrity. Other main related concepts, conditions and aspects of the two are sensitivity, discretion, criticality, concealment, secrecy, privacy, seclusion, isolation, etc.

Confidentiality and Integrity violations are not limited to intentional attacks. Human error, oversight, or ineptitude accounts can lead to his. Confidentiality and integrity must insure the third principle: the availability. It means that authorized subjects acting on what they have right to do are granted timely and uninterrupted access. It should imply granting timely and geographically, uninterrupted accessibility. The three combined allow authentication, authorization and accountability services [1].

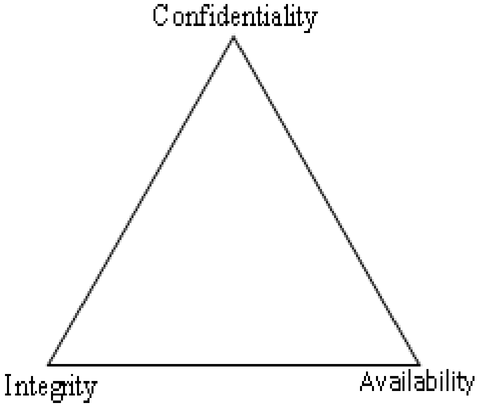


Figure 1. Main Principles of Information Security

## III. RELATED WORKS ON SECURITY ISSUES IN SOCIAL NETWORKS

Due to their complexity and sensitivity, security issues in social networks are addressed by several researchers in regard to find a way to make them safe and secure. Although, dangers inherent to the web and networks are still.

In their paper [2] authors Sattikar and Kulkarni, they namely expose brief contents of 28 papers on security issues in social networks. They all remind the need of searching better solution to ameliorate and or innovate existing methods and techniques. They address security issues and pose foundation of their research using Artificial Intelligence techniques such as Neural Network, Decision Tree techniques, Expert Systems and Adaptive Network based Fuzzy Inference System.

Michael Backes, Matteo Maffei and Kim Pecina in [3] addresses security issues in social networks by proposing new cryptographic framework to secure users. Among some key elements; they work on pseudonym, revocation and other aspects. They analyze Verification of Access Control and Secrecy Properties. They evaluate Attacker model and privacy properties assuming Zero-knowledge proofs as anonymous signatures. Then they implement a subsequent algorithm. In [4] Adu Michael K, Alese Boniface K and Adewale Olumide S. propose a design to authenticate and uniquely identify every internet user. They focus on social networks to fight related cyber criminality. In [5] authors in their time, presented what they considered to be unique security and privacy design challenges brought by the core functionalities of online social networks. They also emphasized on some opportunities of utilizing social network theory to mitigate conflicts occurring in traditional and new designs of social networks.

Papa Nikolaou Alexandros; Ilioudis Christos; Vlachos, Vasileios and Chatzimisios, Periklis in [6] present privacy issues in social networks demonstrating possible breaches in user privacy. They give some examples of real incidents with consequences and various realistic countermeasures.

Other authors explore and expose different techniques and methods which can help to safety, security, privacy and confidentiality on social networks. And this serves as well as directions and foundation for future research where we need to respect and to protect user privacy [7].

## IV. BREACHES AND THREATS IN SOCIAL NETWORKS

### A. *From Attackers and unawareness of users*

Social networks are victims of different types of breaches and attacks mainly by exploiting account hijacking sometimes with high consequences like in case of identity theft. Voyeurism - in case of visibility of purely private information, undue sharing of sensitive information to strangers, unwanted use of data for advertising or electoral, political purposes. This is due to weakness of security, and the complexity of long texts of safety and privacy tips or clauses of confidentiality. Users usually just accept without reading them. Other threats also include, de- anonymization attack, neighborhood attack.

Attacks on user’s profile and personal information including leakage of information through poor privacy settings. Also exist leakage of information to third party application or domain, existing profile cloning, cross-site profile cloning. Social phishing, spam issues or attacks including spam attack on social networking sites, email-based spam attack on social network users, broadcast spam and context-aware spam. HTTP session hijacking, malware spreads across social networks, including fake profiles, social network API, drive-by download attack, shortened and hidden links, cross-site scripting attack, clickjacking. Also physical threat is another issue that social network users need to concern and pay attention [9] [10].

### B. *From legitimate actors*

Less evoked are the following questions: what owners of social networks do they do with information of their users? Legal and legitimate actors in social networks, are they trustworthy and enough loyal towards users on users' information they host? Recently, the scandal case Facebook and Cambridge Analytic is revelator [11]. Rather than a beneficiary of technologies, the social networks users and their information are also products to be sold when known and hidden interests come in.

## V. MAIN SOCIAL NETWORKS IN THE WORLD

Different social networks and Web 2.0 comprises of social networking sites.

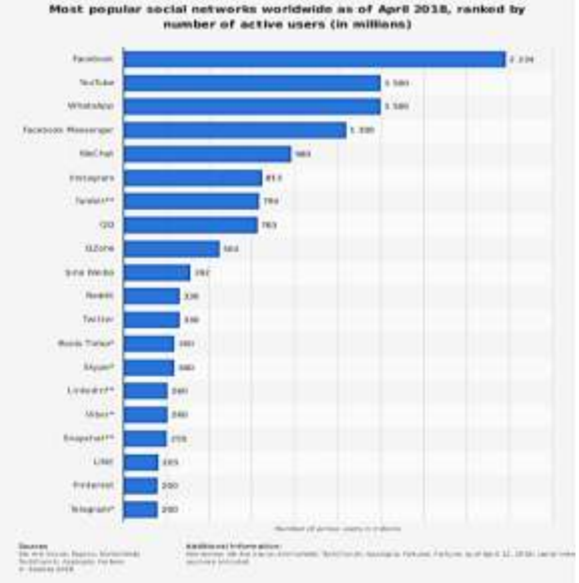


Figure 2: Social Networks by number of active users

Among most known and used social networks are Facebook, YouTube, WhatsApp, WeChat, LinkedIn, Twitter, Google+, etc. The figure bellow show 2018 statistics of users by social networks [8].

### A. *Online Authentication Techniques*

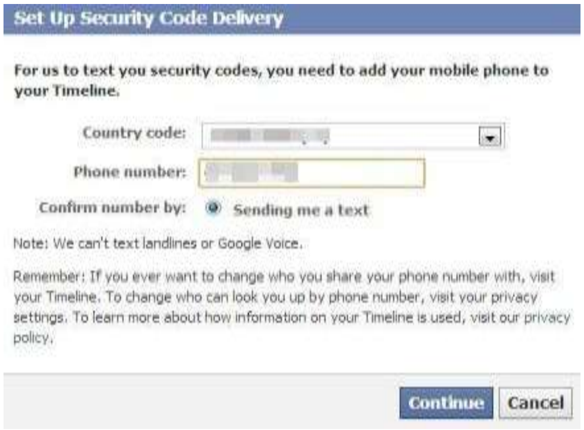
Even if Knowledge-based authentication techniques are still common, some other techniques have been designed and developed. Authentication is no longer just relying on the user to provide only a password at the login prompt. Other mechanisms to make extremely difficult for attackers and their intentions in stealing authentication information and reuse.

Technological and business companies developed different techniques to make safer their interactions and transactions done by their users and in internal management. Among them are banks, administrations, intelligence services, etc. [12] [13].

Four main types of authentication available are: Password based authentication, Certificate based authentication, E-Token based authentication and Biometric based authentication. It can be pseudonymous authentication, relation authentication or anonymous authentication. Also among those techniques to protect users, social networks propose techniques of authentication and rules of managing personal information and online activities and on devices they use to access social networks.

### B. *Using Phone As An Authentication Factor*

As said previously, among techniques and possibilities given to users to secure their accounts, there are based on authentication and tips in managing one's privacy and confidentiality. Authentication is realized by using passwords and sometimes multi-factor authentication [14] [15] [16].



Set Up Security Code Delivery

For us to text you security codes, you need to add your mobile phone to your Timeline.

Country code: [redacted]

Phone number: [redacted]

Confirm number by: ● Sending me a text

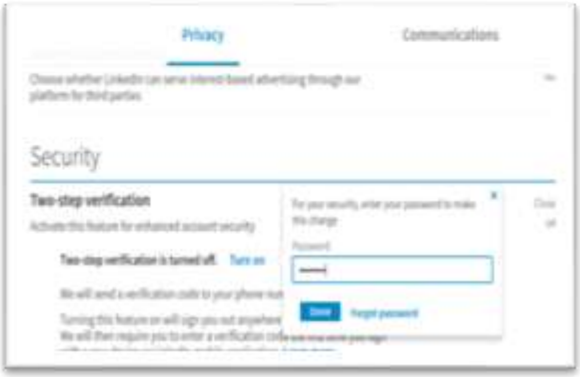
Note: We can't text landlines or Google Voice.

Remember: If you ever want to change who you share your phone number with, visit your Timeline. To change who can look you up by phone number, visit your privacy settings. To learn more about how information on your Timeline is used, visit our privacy policy.

Figure 3: Facebook 2FA Using Mobile Phone

In fact, two-factor authentication is an extra layer added for more security and true authentication. The three following figures show 2FA successively on Facebook the most popular social network in the world, on LinkedIn social networks for professionals, and on MBAEX, a specialized company in block- chain exchange, using Google account and WeChat Q-R Code scanning. Here we focus on multi-factor authentication mainly using mobile phone.

This lead to almost four or five inconveniences: roaming not easy insure for many, lateness of code from the system, the cost related to exchange of OTP-code, SMS-Security, knowing that content passing through some known signal even if "protected" can be intercepted by well-equipped third party. Generating OTP-code for future means storing sensitive information by the way exposing oneself to threats.



Choose whether LinkedIn can serve interest-based advertising through our platform for third parties

Security

Two-step verification

Activate this feature for enhanced account security

Two-step verification is turned off. Turn on

We will send a verification code to your phone nu

Turning this feature on will sign you out anywhere
We will then require you to enter a verification code

For your security, enter your password to make this change

Password

Done Forgot password

Figure 4: LinkedIn 2FA Using Mobile Phone

Figure 5: Google 2FA Using WeChat on MBAEX [17]

In examples in figures above, message codes are sent to a phone number. Another way can also be by push on the phone when trying to connect one's account from another device. [18].

*i. 2FA Using Phone: Advantages*

It has been recognized that two-factor authentication (2FA) improved security in authentication as it verifies user by permanent possession of his phone combined to his password.

Two factors: first something user knows and second something user has and owns. Moreover, the second is a One Time Password (OTP). It's supposed that, even if someone else has user's password, third party cannot access account as long as the phone is user's hand. As an add, already existing security in telephone and mobile and or wireless technologies [19].

***ii. 2FA Using Phone: Limitations***

The first problem and main one is related to mobility. Phone needs signal and connection to networks to continue receiving SMS-code whenever user changes telephone zone area. In some case, even if user is in international rooming, sometimes he is denied access as the system in top of the authentication process can't recognize or is not informed of mobility of user. Secondly, losing his phone can also mean losing one's identity and related accounts.

Alternative methods are proposed such as based on artificial intelligence but also falls in what is known and what someone has. What is known can be a fixed data, maybe a sensitive information user provided already as part of his identity. Or it can be information on activities like identifying friends or last conversations on Facebook, or last used passwords. In sum, this is again giving social networks and potential attackers more information user shouldn't give.

## VI. CONCLUSION AND FURTHER RESEARCH

Social networks play a key role in lives of their users. During this decade, they count billions of active users in different aspect of daily life, professional, familial and friendly relationships, and so on. Social networking sites and applications also have become a potential target for attackers hunting sensitive information provided by users on them.

Most of time, attackers are usually experts than users and will always make victims. Social network security mechanisms have been strengthened but still they have their weakness. Many users do not master good habits and tips to set up their safety, privacy, security and reduce their vulnerabilities. And some cases, attackers use social networks as a channel to spread malware, as they surf on billions of interconnectivity of users involving different properties and attributes. Another aspect is what owners of social networks do they do with information of their users. Recent scandal case involving Facebook and Cambridge Analytical is revealator. Rather than a beneficiary of technologies, the user is also a product to be sold when know and hidden interests come in.

In fine, privacy and security issues in online social networks go increasing and expanding as the number of users continue to increase and information they leave on them. This survey paper addressed different privacy and security issues, name different types of threats and attacks perpetrated online. We also exposed about some techniques to keep a certain level of safety. In further research, it would be useful thinking and designing new techniques on strengthening existing mechanisms to improve security in social networks. Techniques which can be permanent and not limited to geographical use like extending two-factor authentication to mobility. It implies also ethical aspects on behalf of users, third parties and as well as owners of social networks.

## REFERENCES

**1**. J. M. Stewart, M. Chapple and D. Gibson, Certified Information Systems Security Professional, Official Study Guide, Seventh ed., Indianapolis: John Wiley & Sons Inc., 2015.

**2.** A. A. Sattikar and R. V. Kulkarni, "A Review of Security and

Privacy Issues in Socail Networking," *International Journal of Computer Science and Information Technologies*, vol. 2, no. 6, pp. 2784-2787, 2011.

**3.** M. Backes, M. Maffei and K. Pecina, "A Security API for Distributed Social Networks," in *Proceedings of the Network and Distributed System Security Symposium, NDSS 2011*, San Diego, California, 2011.

**4**. M. K. Adu, B. K. Alese and O. S. Adewale, "Mitigating Cybercrime and Online Social Networks Threats in Nigeria," in *World Congress on Engineering and Computer Science 2014 Vol I*, San Francisco, 2014.

5. Z. Chi, S. Jinyuan, Z. Xiaoyan and F. Yuguang, "Privacy and Security for Online Social Networks: Challenges and Opportunities," *IEEE Network.*, vol. 24, no. 4, pp. 13-18, 2010.

**6.** A. Papanikolaou, C. Ilioudis, V. Vlachos and P. Chatzimisios, "Privacy issues in social networks.," in *Social Network Engineering for Secure Web Data and Services, Chapter: 8*, Hershey, IGI Global, 2013 , pp. 162- 183.

**7.** D. Hiatt and Y. B. Choi, "Role of Security in Social Networking," *International Journal of Advanced Computer Science and Applications, (IJACSA)* , vol. IV, no. 2, pp. 12-15, 2016.

**8.** Statista, "Most famous social network sites worldwide as of April 2018, ranked by number of active users (in millions)," © Statista 2018 , 12 April2018. [Online]. Available: https:// www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/. [Accessed 14 06 2018].

**9**. D. Gunatilaka, "A Survey of Privacy and Security Issues in Social Networks," 28 November 2011. [Online]. Available: http://www .cse. wustl. edu/ ~jain /cse571-11/ftp/social.pdf. [Accessed 13 06 2018].

**10**. B. Collins, " Privacy and Security Issues on Social Networking," 10 March 2018. [Online]. Available https:/www.fastcompany. com/1030397/ privacy-and-security-issues- social-networking. [Accessed 14 June 2018].

**11.** K. Granville, "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens," The New York Times, 19 March 2018. [Online]. Available: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge- analytica-explained.html. [Accessed 16 June 2018].

**12.** R. D. Pietro, G. Me and M. A. Strangio, "A two-factor mobile authentication scheme for secure financial transactions," in *International Conference on Mobile Business, 2005. ICMB 2005.* , Sydney, NSW, 2005.

13. A. Fadi, S. Zahidi and E.-H. Wassim, "Two Factor Authentication Using Mobile Phones," in *IEEE/ACS International Conference on Computer Systems and Applications, 2009. AICCSA 2009.*, Rabat, 2009.

**14.** Privacy_Rights_Clearinghouse, "Social Networking Privacy: How to be Safe, Secure and Social," Privacy Rights Clearinghouse, 01 December 2017. [Online]. Available: https://www.privacyrights.org/consumer- guides/social-networking-privacy-how-be-safe-secure-and-social. [Accessed 14 June 2018].

15. K. Abhishek, K. G. Subham, K. R. Animesh and S. Sapna, "Social Networking Sites and Their Security Issues," *International Journal of Scientific and Research Publications,* vol. 3, no. 4, pp. 1-5, April 2013.

**16.** ISACA and CRISC, "Social Media: Business Benefits and Security, Governance and Assurance Perspectives," 26 May 2010. [Online]. Available: http://www.isaca.org/Groups/Professional-English/security- trend/GroupDocuments/Social-Media-Wh-Paper-26-May10- Research.pdf. [Accessed 17 06 2018].

**17**. MBAEX, "Binding Two-Factor Authentication(2FA) Guide," MBAEX, [Online]. Available: https://yka2c3d8902ff4abc934973b0f2b502b01141d32d25a0c8283 64dbf 6dd40613.mbaex.com/about/index.html?id=64. [Accessed 14 June 2018].

**18**. C. Summerson, "How to Set Up Google's New Code-Less Two-Factor Authentication," How-To Geek, 24 June 2016. [Online]. Available: https://www.howtogeek.com/260369/how-to-set-up- google%E2%80%99s-new-code-less-two-factor-authentication/. [Accessed 14 June 2018].

**19.** M. H. Eldefrawy, K. Alghathbar and Muhammad Khurram Khan, "OTP- Based Two-Factor Authentication Using Mobile Phones," in *Eighth International Conference on Information Technology: New Generations (ITNG), 2011*, Las Vegas, NV, USA, 2011.

**20**. C. Bernier, "Multi-Factor Authentication… the simple way," Microsoft TechNet, 02 December 2013. [Online]. Available: https://blogs. technet.microsoft.com/cbernier/2013/12/02/multi-factor-authentication-the-simple-way/. [Accessed 11 June 2018].
*Image Technology and Internet Based Systems, 2008. SITIS '08.*, Bali, Indonesia, 2008.

**21**. A. P. Sabzevar and. A. Stavrou, "Universal Multi-Factor Authentication Using Graphical Passwords," in *IEEE International Conference on Signal.*