Network Security in Modern Society

Vulnerabilities and Countermeasures Taken in Online Social Networks (OSNs)

Tay Wei Jian
School of Computing, Faculty of Engineering
Universiti Teknologi Malaysia
Johor Bahru, Malaysia

***Abstract*—This article discussed current network security in modern society especially in online social networks (OSNs) that have been used by modern society for a long time. The main target online social network of this article is Facebook. Current vulnerabilities of Facebook along with their impact on Facebook authority and its users are discussed in the following article. Besides, current countermeasures taken by Facebook to fight against these malicious contents and the reasons for these countermeasures can tackle security problems to a certain degree will be discussed. The paper also recommended the future direction of research to have a deeper understanding of the vulnerabilities of OSNs and a more effective way in solving the malicious activities caused by vulnerabilities OSNs.**

network security; vulnerabilities; countermeasures; online social network; Facebook

I. INTRODUCTION

Network consists of multiple devices ranging from as small as two devices only to as enormous as billions of devices that have communication with each other. The online network has become an important part of our daily life along with the progressive advancement in communication technologies. For instance, online social networks (OSNs) such as Facebook founded by Mark Zuckerberg and Twitter co-founded by Jack Dorsey, Noah Glass, Biz Stone, and Evan Williams that have been overwhelmingly used and familiar by modern society. According to Statista, over 2.74 billion monthly active users recorded on October 29, 2020.

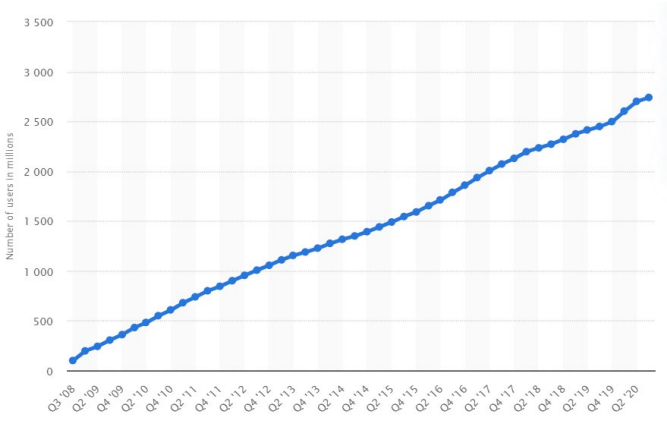

Figure 1: Number of Monthly Active User Worldwide as of 2nd Quarter 2020

(Source: J. Clement, Statista)

Although these networks have accompanied us for a long time, the potential threats, security problems, and privacy challenges proposed by the usage of these networks are considerable and cannot be neglected. For example, more than 300 million Facebook user personal information such as IDs, names, and phone numbers leaked due to database exposure by criminal group start from December 4, 2019, to March 4, 2020. This incident proved the importance of network security. Network security is an act of preventing unauthorized intruder's attack into a certain network. The importance of network security is to protect network users' privacy and their privilege to prevent their personal information being leaked and exposed to dangers and malice when they are using the network services provided. However, opportunities of a network being penetrated still exist although numbers of network security countermeasures had been taken. This is due to the fact of existing flaws and vulnerabilities in the current network causing an enormous amount of hacking and privacy stolen incidents happened in modern society. This article mainly presented about the current network security issues and the current countermeasures taken to solve the present OSNs vulnerabilities.

II. VULNERABILITIES IN OSNS

Facebook is one of the mainstreams in current Online Social Networks (OSNs) due to its popularity. However, there exist some vulnerabilities on Facebook in terms of security and privacy protection.

A. DDoS Attack through File Sharing

Social media like Facebook can be easily attacked or exploited through Distributed Denial of Service (DDoS) attack. [1] Distributed Denial of Service (DDoS) attack occurs when there exist multiple devices of systems occupy the bandwidth or resources of a target system. [2] DDoS attack among social media was usually caused when social media users access files, images or links contained malicious application which generates self-executable files on the users' devices. There are billions of Facebook users share files, images, and download links every day and there is extremely high potential these sharing may contain malware. Therefore, the hidden executed files will be planted and installed in users' devices when they try to access the corrupted files. Furthermore, these corrupted devices will spread the malware into the whole system and affected more victims by generating harmful files when running a malicious application on Facebook. The successful DDoS attack will result in no one can access the system or server down.

B. Information Leaked through Applications

Facebook provide a variety of applications to users. Most of these applications are provided from third-party vendors outside of the Facebook authority. These applications usually requested the users to authorize the access of third-party to users' Facebook account information. The information requested by the third parties usually far more than the information they needed for the users to access the applications and services they provided. [3] This phenomenon caused the private information such as users name, contact number, birthday, address, email address etc. that supposed to be provided for Facebook usage only leaked to third-party. Furthermore, they can even have the access to their friend's information because of the friend list feature provided by Facebook. Therefore, user's privacy is no longer secured by Facebook because the information had been leaked to third-party vendors and there exists the potential of data being stolen from there if the security and countermeasures taken by the third-party vendors are vulnerable, ineffective and incomplete. Millions of relevant user's data collected by Facebook might be exposed to dangers when a single attack targeting the vulnerable third-party occurred. Due to the access given to these third-party applications, these applications usually become the target of hackers to steal the private information of Facebook users. Besides, some applications contained in-app purchase. The purchase made in the applications required the buyers to provide information on credit card or debit card. Card information will be easily leaked if the security measures taken by the third-party developer is ineffective and contained serious flaws. As a result, the users might suffer massive loss in finance if a hacker successfully hacks into the application and acquire the information provided by users.

C. Puppetnets

Puppetnets exploit the design principle of World Wide Web. Web pages can include links to elements from different domains. A network perpetrator can create a specialized web page that contained links that linked to the victim site. The victim site's bandwidth will be consumed enormously when there exists user clicking into the specialized web page because it will force the user to start downloading the materials from the victim website. [3] These Puppetnets can be spread by hiding the link among advertisement and campaign posted on Facebook to attract Facebook users to access the link. However, there are other ways for the Puppetnets being spread on Facebook. For instance, the application provided by Facebook like games. These applications attract most of the Facebook users and prompt the users to invite their friends or share their highest score to attract the user's friends to use the same application they used. An application developer can intentionally create a malicious program or application that contained hidden files or hidden executable code that will cause the application users host and share these files without their notice. This can be used to create a Distributed Denial of Service (DDoS) attack. However, the effect is not limited to DDoS attack only. They can be used to other illegal activities such as host scanning, malware propagation and attacking web pages that using cookie.

D. Authentication

OSNs like Facebook provide two-factor authentication feature which enhances the security protection of their user security. This feature is mainly about providing second protection to users account beside the password set by the users. Basically, this authentication works when there is an attempted login from a device or browser that does not recognize by Facebook authority based on user's recent login devices, the login does not require the users provide the password they set only but also require users to enter a verification code that sent to the users via authentication app or text message (SMS). The common examples of authentication app are Google Authenticator and Duo Mobile. The users can select the security method they want from using authentication app or text message (SMS). Furthermore, users can use text message (SMS) as the verification of their identity and second way to login into their account. However, there is a serious flaw discovered in June of 2013. A security researcher, Jack Whitten discovered that a hacker could modify users' information, for instance, users SMS verification contact number and then request for a password reset. As a result, the verification code will be sent to the hacker's phone instead of the victim's phone due to the change in information. The attacker can use this verification code to change the existing password set by the user without being aware by the user. [3] Although this flaw had been fixed by the on 28 May 2013, there is no guarantee that similar incident happened due to the current unaware flaw existed in Facebook authentication feature.

E. Information Misused through OSNs Profile

Users of online social networks especially Facebook users are willing to fill up their personal information such as birthday, current address, and current location. Furthermore, they are excited to share their daily life by posting their feelings, images, and videos in social media. Although users can set the privacy setting by selecting the visibility of post and personal information, there are still users allow the information visible to the publicity because of the default setting provided by Facebook. [4] A perpetrator will acquire an opportunity to analyse a user's daily life and commit a crime when they identify the opportunity. For example, the potential criminal can identify a vulnerable target through the information of the Facebook users such as daily routine and home address. Therefore, they can use the information acquired to plan a perfect crime to the victim. This kind of information misused is always related to physical harm to the victim. Apart from that, the information misused through Facebook Profile can be used in other illegal activities. Misused information can be associated with the fake profiles and identity theft. Fake profiles usually related to defame or humiliate other users, and as a fake account used to perform illegal business and activities to prevent being caught by the law enforcement authorities. Besides, fake profiles can be used to perform scam on the victim's family, friends and people who close to them. The fake account filled with accurate information of the victim created will be used to add

the victim's friends from the friend list and then tried to perform scam on those who accepted the friend request. This is because the trust between the victims and their friends highly elevate the success rate of scam. [3] The target victims of fake profiles are not limited people who close to the users whose information stolen and misused, but also can be strangers through online shopping scams and romance scams. According to the Federal Trade Commission (FTC), there are nearly $117 million losses reported in just the first six months of 2020 in social media. Fake profiles will elevate the scams performed in social media every year because the perpetrator can escape from the law enforcement authorities and dump the fake profile easily after their scams being identified and reported to the authorities. They will use another fake profile and perform scams to the innocent social media users, for instance, Facebook users to acquire benefits from illegal ways. According to Statista, there were almost 1.5 billion fake Facebook accounts removed in Quarter 2 of 2020.

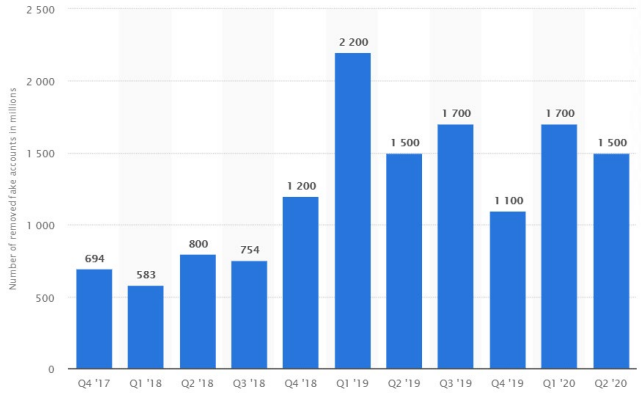

Figure 2: Global Number of Fake Accounts Taken on by Facebook from 4th Quarter 2017 to 2nd Quarter 2020

(Source: J. Clement, Statista)

Besides, these malicious accounts can be used to spread malicious contents and links. These malicious contents can be but not limited to virus and malware that will harm the users who click into it. [5]

F. Other Malicious Activities

There are many cybercrimes can be performed in an online social network, for instance, Facebook. These cybercrimes can be but not limited to phishing, spamming, malware propagation and cyberbully. [6] The most common and easiest to be neglected malicious activity is cyberbullying. In a study, there is nearly 40% of the sample respondents reported being victimized and nearly 25% of the respondents reported perpetrating online harassment. [7] Cyberbully is a malicious activity that can be conducted by a hacker or non-hacker user. Cyberbully usually happened due to low self-control, internalizing traits, psychopathic and Machiavellian traits. [7] These activities usually can cause psychological damage to the users that being defamed and bullied. Although this kind of malicious activity usually associated with psychological damage to the targeted victim only and not involving financial losses, however, this malicious activity also causing problems to the OSNs operators by damaging the reputation of OSNs and users that being victimized. A serious consequence that cannot be denied is leading to the victims cannot overcome the depression caused by cyberbullied and commit suicide. Rumour is another problem existed in OSNs. [6] Rumour can be defined as the distribution of incorrect information, unconfirmed information and manipulation of information causing users who read it have misunderstanding and misled by the incorrect information. [6] These rumours are usually used to damage the reputation of certain authority, company even individual. [6] Phishing is a malicious activity conducted to lure the potential victim for personal or confidential information of the victim. [8] The common phishing type performed in OSN like Facebook is clickjacking by tricking Facebook users to like a page on Facebook, perform a transaction through PayPal or credit card, allow access to camera and microphone to steal users personal and private information. [8] This circumstance will lead to confidential information such as credit card or debit card information leakage, private information leakage and privacy insecure. Besides, fake accounts and spamming activities also can be seen in popular OSN like Facebook. A Facebook statistic from 2012 revealed that out of 83 million fake Facebook accounts, there were 1.5% of those accounts are used to perform spam and other malicious activities. [9] Spamming activities commonly associated with spreading mean and nasty content that could be through a post, message or even friend request also considered as a medium to spread spam. [9] Spam can be defined as interaction and information that the victim never wanted. [9] Spamming activities not only can lead to significant harm to users by infecting users' devices but also consume network resources. Apart from that, spamming activities also may lead to misunderstandings and misleading by users towards current issues by directing users to a website that have no relation with the topics the users seek. [6] Malware propagation usually can be associated with spamming activities by spreading malicious applications, links to the users. Malware is usually designed to do damage and harm to webpage or users. [6] For example, Koobface malware had been distributed to users by using the malicious link on Facebook in 2008. [5] This kind of malware will infect the users' electronic devices causing users participating in illegal activities without their notices. Compromised account is also a kind of malicious activities that can be seen in OSNs like Facebook. Compromised accounts are legitimate user accounts that are created by their own owners but hacked by a third-party resulting the accounts are not only used by the owners only. [4] These compromised accounts had been established complete social connections in online social network and these kinds of accounts can be used to perform scam on the victims' friends. Apart from that, these accounts could damage the reputation of the system through promoting unwanted content causing spam activities in OSNs. [4] Furthermore, these accounts can be used to spread malware and causing millions of OSNs users affected.

III. Current Countermeasures Taken

There exist flaws and vulnerabilities in Facebook, however, the Facebook authority also prepare necessary countermeasures to prevent and solve cyber-attack problems to a certain degree.

A. Two-factor Authentication (2FA)

As mentioned earlier, OSNs like Facebook introduced two-factor authentication method to ensure the security status of Facebook account after its founder, Mark Zuckerberg's account being hacked. Two-factor authentication greatly enhances the security status of users accounts by requiring the users to log in with two verification codes which are their own password and a verification code sent to users via authentication app or SMS. [3] This authentication is more secured if the users decided to use authentication app instead of using SMS. This is because the verification codes are relying on the carrier if using SMS compared to the verification codes is staying with the authentication app if using an authentication app. Hackers can trick carriers by porting the phone number used for authentication to a new device and the authentication code will be sent to the new device instead of to the phone of the users. In contrast, using an authentication app is more secured than using SMS in two-factor authentication. Furthermore, the codes expire quickly, therefore, the hacker would not have sufficient time to complete hacking. By using two-factor authentication, the privacy and security of the users' accounts will be greatly elevated because of the lower possibility of the account being hacked by malicious network users.

B. Privacy Policy

OSNs like Facebook also provide privacy settings accessibility to its users. The users can customize the privacy settings themselves. [10-12] For example, users can customize the visibility of their personal information such as contact number and email address used to the public, friends or no one other than themselves. By setting it to selection besides public would elevate and strengthen privacy protection. Hacker could not obtain a user's personal information by using a stranger account if user set their privacy settings to friends only. Furthermore, the hacker could not access the user's information even though they successfully hacked into user's friends account if the user set the privacy settings to only me. Apart from that, users also have the right to change their account visibility to the search engine such as Google, Yahoo and Bing. By selecting this setting to "No" will greatly decrease the vulnerability of user's account. This is because a malicious network user could not target their victim by using a search engine only, they need to create a Facebook account to find a potential victim. Besides that, Facebook users can decide the visibility of their posts as controlling the visibility of their information. [11] The users can control who can see their posts and apps activities to make their account as much private as possible. Users' privacy can be protected if the users set their privacy settings as lower visibility as possible.

IV. Future Direction

Possible future research direction is including the information about the privacy leakage and its associated risks and harms towards users when online social networks (OSNs) work as a Web tracker. There are many applications and websites approve login via OSNs account. This phenomenon allows OSNs to track their users in a third-party website through cookies. In such situation, OSNs might gather more detailed information about the users and elevate the potential risk of users' privacy information being leaked to hackers through cyber-attack to the OSNs.

Apart from that, more specific detail on current countermeasures taken by OSNs should be included as future research to identify current weaknesses in countermeasures taken against cybersecurity crime. There is scarce information about the current actions taken by OSNs against malicious activities such as fake account, spam, and phishing.

Besides, there is limited information and research on current OSNs' automatic detection system's functions and its effectiveness in detecting malicious accounts and activities in OSNs. The information can be used to identify the current shortcomings in the detection system to improve in detecting cybercrime and solving cybersecurity problems.

Another future research direction is targeting other OSN besides Facebook such as Twitter, Reddit, and Instagram to acquire more information about the vulnerabilities that can be exploited by a hacker and harm the social network's users. Besides, countermeasures that were taken by other OSNs also can be as a reference and example in fighting against cybercrime.

V. Conclusion

There exist flaws and vulnerabilities in current OSNs, especially Facebook. Havocs caused by exploitation on these vulnerabilities not only affecting OSNs users, but also the OSNs provider themselves. OSNs authorities should invest more in enhancing and strengthening security protection to their servers and users' privacy. This is to ensure the benefits of both providers and users are well secured. For example, OSNs authorities can invent and build a more effective automatic detection system in detecting malicious contents and accounts to take necessary actions earlier before the malicious contents spread to users. Apart from that, OSNs users should have awareness and responsibility in managing their own privacy. The users should understand the risks of being targeted by hackers if they did not change their privacy settings to a more secure and safe option. The users also should try to elevate their accounts security level by using a stronger password and two-factor authentication through an authentication app method to decrease their accounts' vulnerability to hackers. Besides, users should reduce their accounts visibility by setting their privacy settings to a more private option to reduce the probability of being targeted by hackers. Both the OSNs authorities and users should take responsibilities in creating a friendly and safe online social networking environment to make OSNs free from cyber-attack.

REFERENCES

[1] Dharmendra Singh, Rakhi Sinha, Pawan Songara, Dr. Rakesh Rathi, "Vulnerabilities and Attacks Targeting Social Networks and Industrial Control Systems", International Journal on Computational Sciences & Applications (IJCSA) Vol.4, No.1, February 2014.

[2] Saman Taghavi Zargar, James Joshi, David Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," in IEEE Communication Surveys & Tutorials, Vol. 15, no. 4, pp. 2046-2069, Fourth Quarter 2013.

[3] Elizabeth Fokes, Lei Li, "A Survey of Security Vulnerabilities in Social Networking Media – The Case of Facebook," RIIT 2014 – Proceedings of the 3rd Annual Conference on Research in Information Technology. 57-62.

[4] Imrul Kayes, Adriana Iamnitchi, "Privacy and Security in Online Social Networks: A Survey," Online Social Networks and Media, Volumes 3-4, pages 1-21, 2017.

[5] Kayode Sakariyah Adewole, Nor Badrul Anuar, Amirrudin Kamsin, Kasturi Dewi Varathan, Syed Abdul Razak, "Malicious Accounts: Dark of the Social Networks," Journal of Network and Computer Applications, Volume 79, pages 41-67, 2017.

[6] Umit Can, Bilal Alatas, "A New Direction in Social Network Analysis: Online Social Network Analysis Problems and Applications," Physica A: Statistical Mechanics and its Applications, Volume 535, 122372, 2019.

[7] Jillian Peterson, James Densley, "Cyber violence: What do we know and where do we go from here," Aggression and Violent Behaviour, Volume 34, pages 193-200, 2017.

[8] Kang Leng Chiew, Kelvin Sheng Chek Yong, Choon Lin Tan, "A Survey of Phishing Attacks: Their Types, Vectors and Technical Approaches," Expert Systems with Applications, Volume 106, pages 1-20, 2018.

[9] Ravneet Kaur, Sarbjeet Singh, Harish Kumar, "Rise of Spam and Compromised Accounts in Online Social Networks: A State-of-the-art Review of Different Combating Approaches," Journal of Network and Computer Applications, Volume 112, pages 53-88, 2018.

[10] Brandon Charles Hoffman, "An Exploratory Study of a User's Facebook Security and Privacy Settings," All Graduate Theses, Dissertations, and Other Capstone Projects. 70.

[11] Johanna Cabalhin, "Facebook User's Data Security and Awareness: A Literature Review," Journal of Academic Research 03:2, pp. 01-13, 2018.

[12] Jennifer Jiyoung Suh and Eszter Hargittai, "Privacy Management on Facebook: Do Device Type and Location of Posting Matter?" published online, July 2015, doi:10.1177/2056305115612783.

[13] J. Clement, "Facebook: number of monthly active users worldwide 2008-2020,", in Statista, 24 November 2020.

[14] J. Clement, "Facebook: fake account removal Q4 2017 – Q2 2020," in Statista, 4 November 2020.