International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Enhancing Social Network Security: A Cloud - Based Approach to Prevent Profile Cloning Attacks

Fahmida Yesmin Chowdhury

Department of Computer Science and Engineering, Faculty of Engineering, University Of Development Alternative, Dhaka, Bangladesh
Email: *fahmida.chowdhury[at]cse.uoda.edu.bd*

Abstract: ***The number of social network users is increasing tremendously. Users are increasingly utilizing social sites for various purposes. Normal users use social sites to connect with their friends and family members, students and teachers use them for study purposes, businessmen use them for their business deals, and sellers also use these social sites for their advertisements. Using these sites, users can easily create new friends and share their interest, feelings, etc. with known and unknown persons which create security holes on these networks and help the attackers to perform different types of attacks. One of the common attacks on social sites is a profile cloning attack or identity theft attack where an attacker creates a similar fake profile of any real user of a social site and does some unwanted tasks acting as that real user. Many research works have been done on the detection of profile cloning attacks. But if it is possible to prevent creating fake profiles or fake profile images then the users of social networks will be more secure. This paper proposed a system to stop profile cloning attacks on all social sites by creating the same standard cloud - based globally verified profile which will be maintained by all social networking sites.***

Keywords: Cybersecurity, Social Networking, Identity Theft, Profile Cloning, Cloud - Based Verification, Profile verification globally

1. Introduction

The place where people can communicate with others to share their opinions or feelings online is normally called a social networking site. Three main categories of social networking sites are social connection, multimedia sharing, and professional. Facebook, Twitter, Google+, and Myspace are the most widely used social connection sites which are mainly designed for various social activities like searching for friends, communicating with old friends, sharing different types of content with known and unknown persons, etc. They are also using social sites for digital marketing, business promotion e - commerce, etc. YouTube and Flickr are now the most popular multimedia - sharing social sites. Many users are now uploading and viewing videos daily using YouTube which helps people to get knowledge on various topics easily. Using Flickr people can share digital images among many persons. LinkedIn is another popular professional social site that is mainly designed for professionals to grow their careers.

According to the paper [1] and information collected from a social networking site [2], the number of Facebook users increased from 901 million to 1.65 Billion from year 2012 to year 2016. This data shows how the popularity of social networking sites is increasing. With this increased popularity, the security risks of these sites are also increasing day by day.

Some security issues which are related to online social networking profiles are mentioned here [3]. Most of the real users use real information and images on their social profiles and it helps the attackers to attack easily to their profiles. Maximum security issues of social sites are created by the unawareness of the users. Currently, Facebook is giving some privacy and security options for their users but many novice users don't know how to apply these features. So when attackers search these types of insecure profiles, they can easily get their personal information and images. By using these data they perform different types of malicious attacks. The way the users can be attacked by social sites is discussed in detail here [4]. Even using strong privacy settings, users' personal information can be stolen by 3rd party applications or domains which are now very popular on social networking sites. Identity theft issue is one of the major security issues of social sites. Profile cloning and social phishing attacks are related to identity theft issue where the attacker acts like any existing real user and use that person's identity for malicious works. Now it becomes easier to perform spam attacks on social networking sites by creating fake profiles of any well - known person. Another important security issue of social sites is malware attacks. In this case, also fake profile creation is one of the easy ways to do malware attacks on a victim's profile. The attacker creates a fake profile of any celebrity and attracts the victim to click on the profile image and spread malware. There are other ways to do malware attacks, such as using social networking API, shortened and hidden links, cross - site scripting, clickjacking, etc. Two well - known malware are Koobface and Twitter worm.

From the above discussion, it is clear that most of the privacy and security issues are related to fake social profiles. So if it is possible to prevent and remove fake profiles from social sites then most of the unwanted issues can be solved and social users will be safe. When every profile of the social sites is verified then it will be impossible for the attacker to create fake profiles and this will reduce maximum malicious activities. Many social networking sites already implemented the option in their sites to verify user profiles but only for celebrities. Many celebrities do not use any online social sites and many of them didn't verify their profile either. This helps attackers create fake profiles on behalf of them. Another point is that many people have multiple social accounts. Using the current profile verification system, they need to verify their profile for each account separately. This paper mainly focuses on creating the same standard cloud - based globally verified social

profile that not only prevents various malicious attacks but also makes the profile verification process easier for social users.

2. Profile Cloning Attack

The profile of any online social media user is now a very important factor for the particular user to perform social activities. In various social networking attacks, profile cloning attack is an important security issue. The attacker creates a fake email account and uses this email address to create a similar fake account using the information of a real social network user on that particular social networking site [5]. After creating this fake social account, the attacker tries to copy everything from the victim's profile to make the fake profile look like the original. With this clone profile, the attacker can gain control of the victim's real profile and perform many unwanted or undesirable tasks which reduces the personal image of the victim's friends.

Profile cloning can be done in two ways [6]. In existing - site profile cloning, the attacker creates a fake profile in the same social site where the real user exists. In cross - site profile cloning, the attacker creates a fake profile in different social sites where the real user account does not exist. Enhancing social users' concerns can make users' information safe and reduce this attack by using social sites' security and privacy settings but many novice users can't apply these settings properly or don't think about the security concerns when adding a friend to increase their popularity on social sites. So it requires other ways to implement for preventing this attack properly.

3. Related Works

Profile cloning attacks can be reduced by detecting existing fake profiles and preventing users from creating fake profiles. Both ways are shortly explained here.

3.1. Detecting fake profile

Detecting and blocking all fake profiles from the social networking site is one option to reduce this attack. Much research has been done on detecting fake profiles. Profile similarity techniques can be applied to social networking databases to identify fake profiles [7]. Here, data are collected from various social networking sites to identify similar profile attributes to select suspicious profiles and verify the real profile by questionnaires and providing any identity proof like government ID.

In the paper [8], fake profiles are detected by three steps which are information distiller, profile hunter, and profile verifier. In the first step, a profile is selected for detecting a fake profile and all identifying terms of that particular user are collected and sent to the profile hunter. This step is used to search all similar profiles on popular social sites by matching selected users' identifying terms and sending the result to the profile verifier. This step calculates the similarity scores between real profiles and collected profiles and detects the fake profiles. However, this technique will not accurately detect all fake profiles of all social sites.

3.2. Prevent malicious users from creating fake profiles or using fake profile images

The best solution to reduce profile cloning attacks is to prevent users from creating not only fake profiles but prevent using fake profile images. If the proper restriction can be implemented during profile creation then the malicious users will not be able to create a fake profile and do harmful activities to other real social users. The most important part of any social profile is the profile image. When any user sends a friend request to another user then the receiving user will make a friendship if he/she can recognize the image or be impressed by the sender's image. Profile verification system can be a necessary step to prevent profile cloning attacks but this can't prevent the use of fake images as profile images. Social networking sites don't set any restrictions in setting other people's images as profile images except for some celebrities. Attackers can easily use this security hole and can try to attack by making friends with the use of fake profile images. Making the profile verification system easier for all social sites and preventing profile cloning attacks by using verified profile data are the main motivations of this paper.

4. Current Profile Verification System

Currently, Facebook provides two types of badges to indicate a verified profile and page after verification but this type of verification is not open for normal users yet [9]. After verification, blue badges are given by Facebook to popular celebrities, media companies, or brands to mention that they are authentic, and gray badges are given to authentic businesses or organizations. Facebook is using its authentication policies to verify profiles or pages. Another popular social site Twitter also provides blue verified badges for renowned public figures, companies, brands, or business organizations [10]. For verification, this site follows some rules and regulations, such as the profile must contain a real user's name, phone number, email, public tweet setting, etc. and the brand or organization must use the real company name, logo, etc. YouTube and many other social sites are using phone verification systems to verify their user's account.

According to the existing verification system, if a single user has different types of social accounts on different social sites then he/she needs to be verified for each account separately by using different rules and regulations. This is more time - consuming and undesirable. There is no common profile verification system for all types of online social users to make the profile verification system easier and make every person's social profile safe and secure.

5. Proposed Profile Verification System

To verify the profile of social users globally, every social site must follow the same standard profile verification system that is proposed in this paper. According to this system, if a social user can verify the profile on any popular social site then he/she will be able to use this information to create a verified profile on other social sites. There are two steps to verify the profile. The first step is to verify the NID information for the NID holder or approve the profile owner

information by any verified NID holder. The second step is to verify the recent capture image by matching it with the NID image or approved by another verified profile owner. If the user can verify both steps then a valid profile code will be given to the user to open any social account in any social networking site as a verified user.

5.1. Profile verification by NID

The user with a NID cardholder has to create a verified global profile with email, image of national ID information and NID associated phone number before creating any social profile. Here user's NID information and NID associated phone number will be used to verify the first step of the verification system.

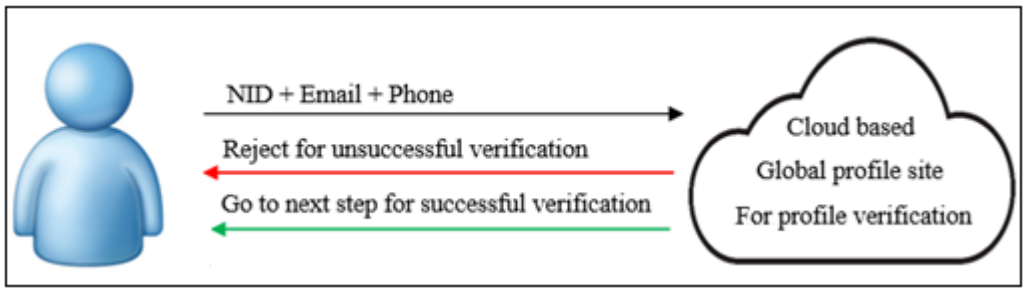

Figure 1: NID verification for NID card holder

5.2. Profile verification by relative's NID

There are many young social networking users who don't have NID to verify them. To verify this type of users, another verification system is proposed in this paper. Young user will send request with real name, email, date of birth, phone no and profile image to any close relative who is globally verified by NID. If the young user is approved by that verified user then he/she will be able to create a temporary verified profile which will be associated with that relative profile and can go for next step.

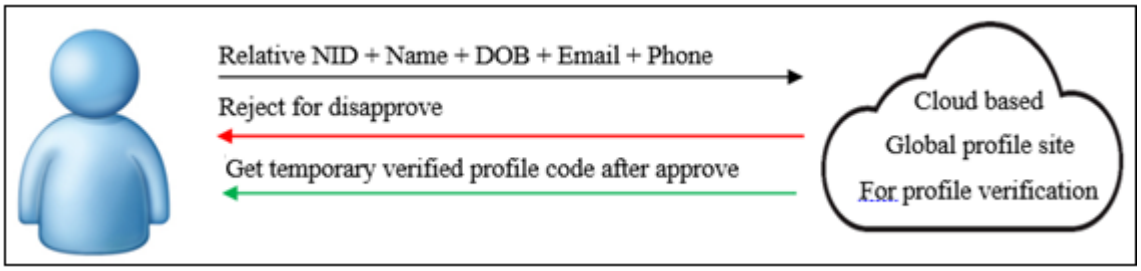

Figure 2: Temporary profile verification by relative NID

5.3. Profile Image Verification

After verifying profile information, if the user is able to use fake image as profile image then the use of this system is totally meaningless. After profile information verification, profile image will be taken by capturing live image and if the NID image and newly taken capture image are similar then that profile will be marked as verified global profile and a unique profile code will be given to the user. Using this profile code user will be able to create account on other social networking site that supports the same standard of verification.

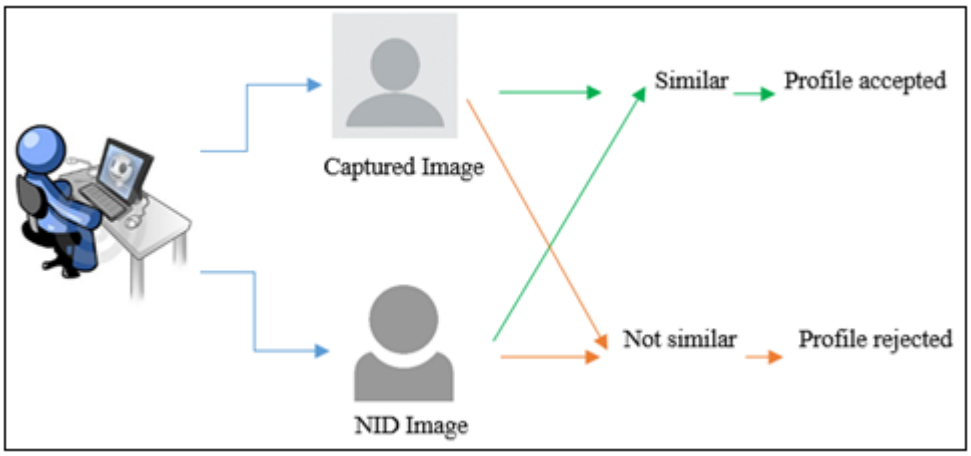

Figure 3: Profile image verification process

For the young social networking users, the profile image must be verified by the captured image and the image approved by the relative who is associated with the young user's account in place of NID account.

5.4. Unique profile code generation

For both permanent and temporary profile code, a passcode will be taken from the user for security and after encryption will be added as a last part of the profile code. After profile verification by NID, profile code will be generated by taking following information of the profile owner. These are,

Birth year - Retrieve from NID
Last four digit of Phone – Used for NID and profile verification
NID No – Retrieve from NID
Profile code = [birth year] - [last 4 digits of phone no] - [NID]/ [R - NID] - [encrypted passcode]

The overall system can be summarized as,

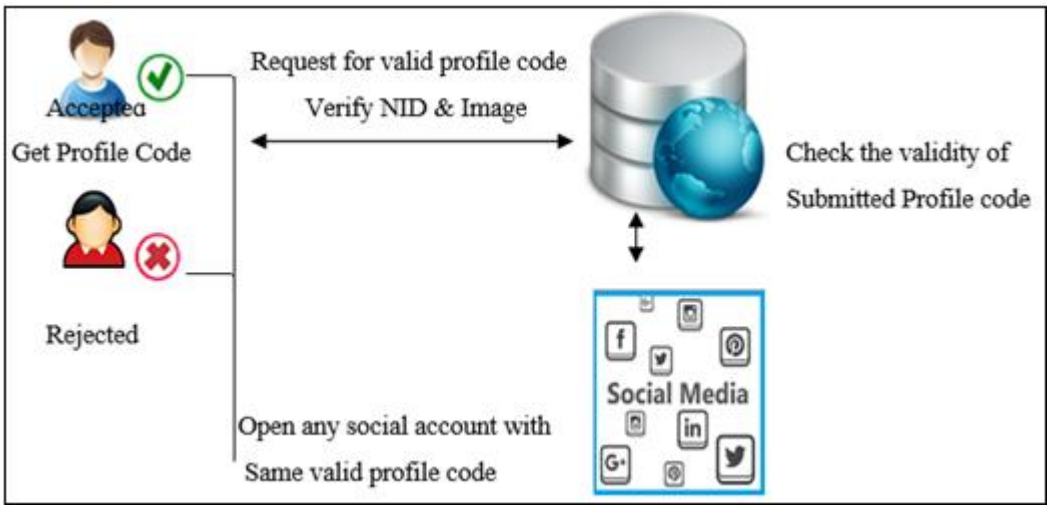

Figure 4: Use of global database to prevent fake social profile creation

6. Benefits of using same standard globally verified profile

To prevent various types of social attacks, profile verification is now very important issue for the social networking sites. Currently many cyber attacks are done by using security holes of these social sites. On 12th May 2017, a cyber - attack has been done on more than 230, 000 computers of 150 countries [11]. This attack is known as WannaCrypt attack. Microsoft windows operating system based computers was affected by this attack. In this attack, all data are encrypted and demands ransom payment for recover. It is assumed that the main reason behind this attack is phishing link. Use of social networking sites help to spread this type of link very fast because many social users normally clicks on the link that shows interesting or attractive topic or image or video as title. All these types of contents are mainly created by using fake profile to spread the malware. So profile validity of social sites is now very important to prevent these attacks.

First benefit of creating globally verified profile is to prevent fake profile creation. NID based phone verification will stop user from using other's information during profile creation. Even though any attacker is able to collect other's NID information, but he/she will not be able to verify the phone number associated with the NID because only NID holder can verify the number. This will reduce the maximum possibility of fake profile creation. And the user will not able to use other image also to verify profile image because profile image will be taken by verifying live capture image.

Second benefit of globally verified profile is that profile owner can use the same profile code for all types of social networking sites and the user doesn't require to verify the identity for each site separately. Using one profile code, user will be able to create verified profile in all social sites like Facebook, Twitter or Linked In without handling any profile verification hassle if all the popular social sites follow the proposed verification system.

7. Demerits of proposed profile verification system

Since the database of the global site will contains all real user's personal information, so the database needs to be more secure to protect the user's personal data from malicious attacks. If the cloud database is attacked by any malicious user then any unwanted occurrence can be happened.

8. Proposed System to prevent profile cloning attack using verified data

All new profiles which will be created by using the proposed system can't be cloned by malicious users or spammers. When a new user wants to create a social profile then he has to create a verified profile in any well - known social networking site. After verification, user can apply any features of social networking sites and changing profile image is one of the common tasks of them. The first step of profile cloning attack is to use fake image or other user's image. Currently all of the social sites give flexibility to change profile image any time by any image and there is no

restriction to use other person's image as profile image. So any user can easily change the profile image later by anyone's image after successfully creating a verified profile with valid data and image. In this way the malicious user will be able to send friend request using fake image to the victim after verification. This activity can be prevented by two ways. One is the image verification process by each social site and other is to send real profile image and name with each friend request to give information about the real user to other users.

8.1. Image verification process

To implement this process every social site must provide a restriction on using other's image as profile image. According to this restriction, user will not be able to use other's image as profile image and the changed profile image must be the real owner's image. So when the user will change profile image then social site will verify this image with the verified global profile image. Well known social site, Facebook already uses image similarity techniques to tag friends. So this process can be easily implemented on social sites. But there are many real social users who don't want to use own picture as their profile image or want to use different type of profile image as temporary image. So this process will not be an appropriate solution for this problem.

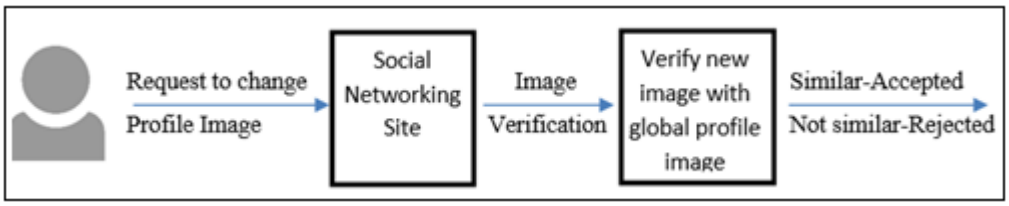

Figure 5: Image verification system to change profile image

8.2. Attach Profile Data with each Request

The other process is to attach real profile image and name which are retrieved from globally verified data. According to this process after creating verified global profile, user can change his profile image by any other image anytime. No need to apply any restriction for changing the profile image or verify the changed image with previous profile image. In this case, when a user changes the profile image by any image of celebrity or any existing real user's image and sends a request to make a new friend then social site will attach requesting user's real basic information such as global profile image and name with every request. So before accepting friend request, the other user will be able to see the real user information and can decide to accept the request or not. Every social site must implement this process in their sites to prevent not only profile cloning attacks but also to reduce many malicious activities from social sites.

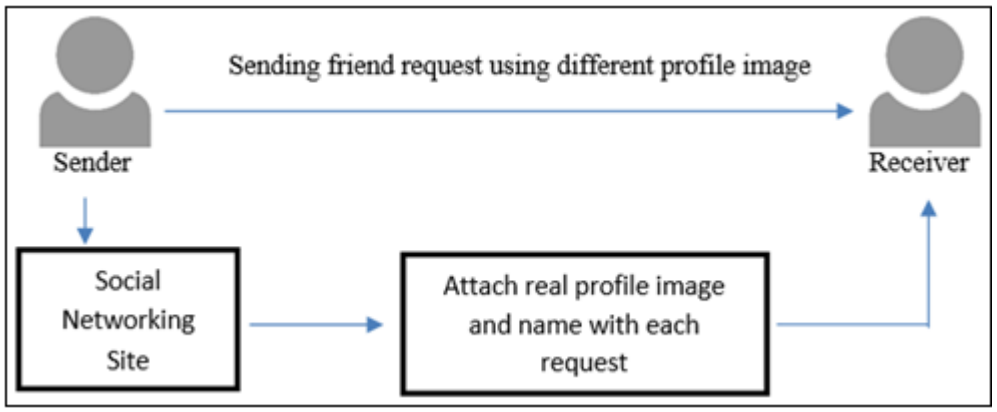

Figure 6: Prevent profile cloning attack by attaching global profile data

9. Conclusion

In current social networking sites, fake profile creation is very easy task because no profile verification process is implemented for normal users. Some restrictions are added for well - known public figures but not for all regions. The proposed system will help to make profile verification system easier not only for celebrities but also for normal real users. All social networking sites give the flexibility to change the profile image of their users any time and when a user send friend request to other user then his/her current profile image is shown. After verifying the profile if any user changed his profile image by a fake image then other users can be confused easily by that image. So it is necessary to consider this issue for social networking sites to prevent attacks by using fake image. Thispaper concludes that implementing a cloud - based globally verified profile system across all social networking sites can significantly mitigate the risks associated with profile cloning and identity theft. This universal profile verification system will promise a substantial improvement in social network security and user trust.

References

[1] Abhishek Kumar, Subham Kumar Gupta, Animesh Kumar Rai, Sapna Sinha, "Social Networking Sites and Their Security Issues", International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013.
[2] https: //www.facebook. com/photo. php?fbid=10102803309152781&set=a.612287952871. 2204760.4&type=3&theater
[3] M. Milton Joe, Dr. B. Ramakrishnan. "A Survey of Various Security Issues in Online Social Networks. " *International Journal of Computer Networks and Applications* (2014).
[4] Gunatilaka, Dolvara. *A Survey of Privacy and Security Issues in Social Networks*. n. d. http: //www.cs. wustl. edu/~jain/cse571 - 11/ftp/social/index. html
[5] http: //www.news24. com/MyNews24/Facebook - cloning - How - its - done - and - how - to - prevent - it - 20130530
[6] http: //www.cse. wustl. edu/~jain/cse571 - 11/ftp/social/
[7] Dr. M. Nandhini[1], Bikram Bikash Das[2], "Profile Similarity Technique for Detection of
[8] Duplicate Profiles in Online Social Network", International Journal of Computer Science and Information Technologies, Vol.7 (2), 2016, 507 - 512
[9] Georgios Kontaxis, IasonasPolakis, Sotiris Ioannidis and Evangelos P. Markatos, "Detecting Social Network Profile Cloning", Pervasive Computing and Communications Workshops (PERCOM Workshops), March 2011.
[10] *What is a verified Page or profile*, https: //www.facebook. com/help/196050490547892
[11] *Request to verify an account*, https: //support. twitter. com/articles/20174631#.
[12] *WannaCry ransomware attack*, May 2017, https: //en. wikipedia. org/wiki/WannaCry_ransomware_attack