SNKnock: A free security tool for Facebook users

Mahmoud Samir Fayed
King Saud University
Riyadh, Saudi Arabia
mafayed@KSU.EDU.SA

Abstract—The Facebook Social network is very famous and widely used by millions of users all over the world. Facebook comes with high level of usability so users can easily find their friends and connect to them, but there are security issues related to this process where the attacker can make same-site or cross-site profile cloning attacks to get other users data. In this paper we will identify advanced same-site or cross-site profile cloning attacks then we will propose a security solution to these attacks where the user must record a voice message and answer some questions when he sends a friend request to another user, and then the other user will listen to this message before deciding to accept or reject the request. We implemented this solution by developing new web application called SNKnock which is available as free service.

Keywords— Social Network; Security; Facebook; Same-site profile cloning attacks; Cross-site profile cloning attacks; SNKnock

I. INTRODUCTION

The social network becomes a famous and well known tool for communication with the peoples which we know in the real world and, The Facebook website is an example of a very successful social network (SN) with millions of users all over the world [1].

During the last years the Facebook social network website becomes a general direction for research by many researchers all over the world. And now there are many studies in different dimensions around the Facebook, for example there are studies in the human behavior [2-9], Psychology [10], business [15-16], decision support systems [17] and security [11-14].

To start using facebook you need to create an account with a username and password, then you start by adding your information (optional) like data of birth, job & photos then you search for your friends by their names or emails [20].

To communicate with your friends you can add them to your friends list and this process requires their permission where you send the friend request and then your friend accepts that request and after that only you can see their posts, photos & links which are set by them to be visible only to the accounts in their friends list [18] Before being a friend you can only see public posts and nothing more. Public posts may include their posts in the group you are joined and/or their comments on the mutual friend’s posts [19].

The problem with this procedure (Send friend Request - then Accept/Reject) are concentrated in the same-site and/or cross-site profile cloning attacks, where the attacker can create an account and put the name of a person known to the victim then send the friend request which is expected to be accepted by the victim because he/she think it’s coming from a person they know then the attacker gets his/her information [11].

If the account created by the attacker is the first account with this name in the same social network , i.e. the real user don’t have account in this social network, then it’s cross-site profile cloning attack which don’t lead to suspicion. But, if the account is duplication to a real account in the same social network then it’s a same-site profile cloning attack which may lead to suspicion and discovered easily.

In this article we will concentrate on the profile cloning attacks and we will identify advanced types of these attacks then we will propose a security solution to this attack.

The structure of this paper is

Section2: Profile cloning attacks and users awareness
Section3: Identification of advanced profile cloning attacks
Section4: The proposed solution
Section5: The implementation
Section6: Conclusion and Future work

II. PROFILE CLONING ATTACKS AND USERS AWARENESS

When the user know about profile cloning attacks he/she can do a check before accepting the friend request, The check done by opening the profile page of the person who sent the friend request and looking at the data to guess is this a real account or not, This could includes for example

- Looking at other information other than the name and the photo, this information maybe information like data of birth, job, city & more photos.
- Looking at the public posts/comments by this user and when he/she joined the Facebook
Looking at comments of other users on the public posts

Looking at the mutual friends

The attacker or the user may hide most of this information and make it visible only to friends. The reason if this is an attacker is to do a trick while if this is a real user he/she may do this for security and privacy reasons. So when the person don’t see enough information he can’t quickly guess is this a real account or not, and may accept the friend request then do another check to look at more information.

After accepting the friend request the vision becomes clearer and the information may be enough to take the decision to keep this user as a friend or to delete it.

Some users may look only at the available information and concentrate on the important ones like the mutual friends and take final decision based on that.

III. IDENTIFICATION OF ADVANCED PROFILE CLONING ATTACKS

Now we will define the advanced profile cloning attack which takes advantage from the next behaviors

1 – Some users may decide to accept or reject the friend request based only on the available information and trust the account based on the mutual friends

2 – The attacker can change the name which appears in the profile

3 – The attack can be done in more than one stage

In the advanced profile cloning attack, the attacker could do the attack in the next stages.

The First Stage (Prepare)

- Create a group of Facebook accounts (using more than one account in the attack is an idea from the Sybil attack [11] which get advantage of the structure of the social network) this group will be called List(1). Look at figure (1).
- Connect these accounts together in a one to many structures where one account will be the head or the center and will be called Attacker (Root) which contains profile page with a lot of posts and comments from other fake accounts.
- Spend some time making a communication between these fake accounts until the Attacker (Root) account seems to be an account for real human have friends and is doing real activities

Fig. 1 The first stage in the advanced profile cloning attack

The Second Stage (Hidden movement)

- Know as much as you can of accounts which is connected to the victim from the friend list (if it’s visible) or by doing a search using names (if the accounts appears in the search results) and this list will be called List(2). Look at figure (2)
  - Use some of the fake accounts and send friend requests to the collected accounts and see if they will accept the friend request or not
    - If Yes
      - Record this account as a weak account, send the friend request directly from all of the fake accounts in List(1) including the Attacker (Root) account to become a friend
    - If you can’t find a weak accounts do the previous procedure with every account in List(2)

The third stage (Grow)

- Repeat stage one and two for more than one time to prepare more than one network Attacker (Root) and List(1) to use in the next stage
- Use your experience from the previous stages to quickly create these accounts and connect it to the accounts in List(2)

The Last stage (Go to the victim)
• Rename the attacker(Root) accounts to a names known by the victim ( use 2 or 3 attacker(Root) accounts)

• Send the friend requests at the same time or one by one (try both if you have many attacker(Root) accounts)

Now the victim will find these accounts carry names known by him/her and there is activity by these accounts and there are real mutual friends. One of these requests could be accepted based on the account name and the relationship between the victim and the real person whose name is used.

The goal from the identification of this attack is to clear that even if the user is aware of the profile cloning attack it’s not enough to check the account before and after accepting the friend request because the attacker can put data and can make mutual friends to let us figure that everything is ok.

We need a more secure system when we accept the friend requests.

![Fig. 2 List(2) collected by the attacker](image)

![Fig. 3 The attacker is trying at first to find the weak accounts in the List(2)](image)

IV. THE PROPOSED SOLUTION

We propose a security solution to the profile cloning attacks. Our proposal is based on character identification through their voice (Something you are).

We will develop a web application and the user who wants to protect himself/herself against the profile cloning attacks will open this web application. The web application will ask the user to determine 2 things as input (email address & questions) then will generate a link which will be the output of the web application.

After that the user will spread this hyperlink to peoples looking to become his/her friends in the social network. When someone would like to become a friend he/she will click on that link then will answer the questions using his/her voice.

![Fig. 4 SNKnock Model](image)
After that an email message will be sent to the original user containing a link to the sound file. The original user will listen to the sound file then decide to accept or reject the friend request.

VE. THE IMPLEMENTATION (THE SNKNOCK WEB APPLICATION)

We implemented our proposed solution by developing a web application called SNKnock[21] which developed using HTML [22], CSS [23], JavaScript [24], PHP[25] & MySQL[26].

The SNKnock user interface is available in two languages (Arabic & English) and the user can change the language using a hyperlink in the bottom of the webpage.

The SNKnock database contains 1 table called Questions
The table contains the next columns

| Index | Column Name | Type          |
|-------|-------------|---------------|
| 1     | Id          | Int (AUTO_INCREMENT) |
| 2     | Email       | Varchar       |
| 3     | questions   | Varchar       |

The user can mix between typing questions and selecting questions from the listbox. The next figure presents a real example demonstrates how to use the service.

The user entered an email address: Alice@test.com Then selected typed one question: Talk to me about myself?

After that the user clicked on the hyperlink: Generate Hyperlink. As a result for this a new hyperlink is generated: http://snknock.sf.net/en/answer.php?code=43. The hyperlink generation process done by the next php source code.
The user now can put this hyperlink in his/her profile page in the Facebook website. The link can be inserted to the about section along with a message like (Please, to be my friend, send the friend request then click on this link and answer my question using your voice, I do that because I would like to avoid fake accounts and profile cloning attacks) or any other message by the user.

When another user or an attacker click on the link he will get a webpage similar to the one in the next figure.

The user or the attacker will see the question and he will answer it using his/her voice. To answer the question he/she will click the button “Record the answer” then will answer the question then will click “Stop recording” and he will listen to his/her answer.

When the user or the attacker click “send the answer” the recorded voice will be saved in a sound file stored on the web server and an email message will be sent to the original user who generated the hyperlink to this webpage using SNKnock.

The questions are displayed by the next PHP code:

```php
<?php
    $str_file = file_get_contents( "header.html" ) ;
echo $str_file ;
include('snknock_db.php');
$con = snknock_db_open();
if (mysqli_connect_errno())
{
echo "Failed to connect to MySQL: " . mysqli_connect_error();
}
$result = mysqli_query($con,"SELECT * FROM questions where id = " . $code . "");
while($row = mysqli_fetch_array($result))
{
echo " <p style='text-align:center'> <font size='4'> " ;
echo " <br />" ;
foreach(preg_split("((
|\n)|(

))", $row['questions']) as $line)
{
echo $line;
echo " <br />" ;
}
echo " </font> </p> " ;
$con = "1" ;
}
if ( $con == "1" )
{
    $str_file = file_get_contents( "voice.html" ) ;
    $str_file = str_replace("THEFILENAMEISHERE", "answerfile_" . rand(1,2000) . rand(1000,2000) . rand(2000,5000) . rand(7000,90000) , $str_file);
    $str_file = str_replace("THEUSERCODEISHERE", $code . $str_file);
echo $str_file ;
}
mysqli_close($con);
?>
```

After that the original user will get an email message, he/she will click on the sound file link which is embedded in the email message to listen to the answer and after that he will decide to accept or reject the friend request.

CONCLUSION AND FUTURE WORK

In this paper we identified advanced profile cloning attacks and proposed a security solution to this type of attack then we
implemented our proposed solution by developing a web application.

We know that there are some limitations to our solution for example some users don’t have mice device to record the sound, some hackers may find a way to pass this voice test, sometimes the Facebook user get friend requests from people known to him but he/she never listened to their voice before.

In the future we are looking to extend our solution by fixing known issues and adding more security options like identification based on web camera and nested questions where the user will get a question based on his answer to the previous question.

REFERENCES

1. Facebook statistics <http://www.facebook.com/press/info.php?statistics>
2. Baiyun Chen and Justin Marcus, “Students’ self-presentation on Facebook: An examination of personality and self-construal factors”, Computers in Human Behavior vol. 28 , 2012, pp. 2091–2099
3. Gabriela Grosscek, Ramona Bran and Laurentiu Tiu, “Dear teacher, what should I write on my wall? A case study on academic uses of Facebook”, Procedia Social and Behavioral Sciences vol. 15, 2011, pp. 1425–1430
4. Khe Foon Hew, “Students’ and teachers’ use of Facebook”, Computers in Human Behavior vol. 27, 2011, pp. 662–676
5. Francis T. McAndrew and Hye Sun Jeong, “Who does what on Facebook? Age, sex, and relationship status as predictors of Facebook use”, Computers in Human Behavior vol. 28, 2012 pp. 2359–2365
6. Khaled Saleh Al Omoush, Saad Ghaleb Yaseen and Mohammad Atwah Alma’aitah, “The impact of Arab cultural values on online social networking: The case of Facebook”, Computers in Human Behavior vol. 28, 2012, pp. 2387–2399
7. Reynol Junco, “Comparing actual and self-reported measures of Facebook use”, Computers in Human Behavior, vol. 29, 2013, pp. 626–631
8. Rachel Grieve, Michaeille Indian, Kate Witteveen and G. Anne Tolan, Jessica Marrington, “Computers in Human Behavior” vol. 29, 2013, pp. 604–609
9. Amanda Nosko *, Eileen Wood and Seija Molema, “All about me: Disclosure in online social networking profiles: The case of FACEBOOK”, Computers in Human Behavior vol. 26, 2010, pp. 406–418
10. Tiffany A. Pempek, Yevdokiya A. Yermolayeva and Sandra L. Calvert, “College students’ social networking experiences on Facebook”, Journal of Applied Developmental Psychology, vol. 30, 2009, pp. 227–238
11. Hongyu Gao, Jun Hu, Tuo Huang, Jingnan Wang and Yan Chen, “Security Issues in Online Social Networks”, published by the IEEE computer society, 1089-7801/11/$26.00 © 2011 IEEE,IEEE INTERNET COMPUTING
12. Mehmet Salinoglua, Aysen Dener Akkayab and David Ange, “Can We Assess and Monitor Privacy and Security Risk for Social Networks?”, Procedia - Social and Behavioral Sciences, vol. 57, 2012, pp. 163 – 169
13. Gail-Joon Ahn, Mohamed Shehab and Anna Squicciarini, “Security and Privacy in Social Networks”, Published by the IEEE Computer Society, 1089-7801/11/$26.00 © 2011 IEEE, IEEE INTERNET COMPUTING
14. Shi-Wei Lin and Yu-Cheng Liu, “The effects of motivations, trust, and privacy concern in social networking”, Springer-Vorlag, 2012
15. William P. Smith and Deborah L. Kidder, “You’ve been tagged! (Then again, maybe not): Employers and Facebook “, Business Horizons, vol 53, 2010, pp 491–499
16. Heman C. Sashittal, Rajendran Siriramachandramurthy and Monica Hodis, “Targeting college students on Facebook? How to stop wasting your money”, Business Horizons vol. 55, 2012, pp. 495–507
17. Rajarshi Chakraborty, Claire Vishik and H. Raghav Rao, “Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing”, Decision Support Systems, 2013
18. Facebook add friends and friend requests <http://www.facebook.com/help/friends>
19. Facebook how to post and share < http://www.facebook.com/help/333140160100643>
20. Facebook create an account <http://www.facebook.com/help/34512135559712>
21. SNKnick website < http://snknock.sf.net>
22. Wikipedia, HTML < https://en.wikipedia.org/wiki/HTML>
23. Wikipedia, CSS < https://en.wikipedia.org/wiki/Cascading_Sheets>
24. Wikipedia, JavaScript < http://en.wikipedia.org/wiki/JavaScript>
25. Wikipedia, PHP < https://en.wikipedia.org/wiki/PHP>
26. Wikipedia, MySQL < http://en.wikipedia.org/wiki/MySQL>