GOCE DELCEV UNIVERSITY - STIP
FACULTY OF COMPUTER SCIENCE

ISSN 2545-4803 on line

BALKAN JOURNAL OF APPLIED MATHEMATICS AND INFORMATICS (BJAMI)

BALKAN JOURNAL
OF APPLIED MATHEMATICS AND INFORMATICS

YEAR 2019

VOLUME II, Number 1

GOCE DELCEV UNIVERSITY - STIP, REPUBLIC OF NORTH MACEDONIA
FACULTY OF COMPUTER SCIENCE

ISSN 2545-4803 on line

BALKAN JOURNAL OF APPLIED MATHEMATICS AND INFORMATICS

(BJAMI)

YEAR 2019 VOLUME II, Number 1

AIMS AND SCOPE:
BJAMI publishes original research articles in the areas of applied mathematics and informatics.

Topics:
1. Computer science;
2. Computer and software engineering;
3. Information technology;
4. Computer security;
5. Electrical engineering;
6. Telecommunication;
7. Mathematics and its applications;
8. Articles of interdisciplinary of computer and information sciences with education, economics, environmental, health, and engineering.

Address of the editorial office
Goce Delcev University – Stip
Faculty of philology
Krste Misirkov 10-A
PO box 201, 2000 Štip,
Republic of North Macedonia

BALKAN JOURNAL
OF APPLIED MATHEMATICS AND INFORMATICS (BJAMI), Vol 2

ISSN 2545-4803 on line
Vol. 2, No. 1, Year 2019

EDITORIAL BOARD

CONTENT

UDC: 004.7.056.5

ACQUIRING INFORMATION USING SOCIAL ENGINEERING

Mladen Kiprijanov, Saso Gelev and Davor Vasielvski
ICT - Information and communication technologies

Abstract. In this paper we will try to describe a new social engineering technique. We name it as acquiring information by using an image. This technique can be used as a power open source tool for acquiring various information from a visitor through the Internet. If we use this technique, with a certain modification in PHP code, we can acquire all the information that can be obtained over the Internet.

1. Introduction

Different habitats, same people but with different characters and attitudes, thanks to the virtual world, everybody can express themselves in their own way and transmit a message hiding his/her identity.

The virtual human world becomes more and more the natural environment in which people daily live and work. In that virtual world and with the help of the four wires (the first, second, third and the sixth wire of the RJ-45 network connector), thanks to the unlimited communication possibilities and access to all information, people realize their own wishes and needs and, at the same time, develop their potentials in a society.

The virtual world, on the one hand, has a lot of benefits, but on the other hand, it also has a lot of negative benefits. The most dangerous negative benefit is computer crime (cybercrime). A new modified version of the classic crime.

The abuse of human being and ICT[1] are more frequent and more dangerous. One of the most used technique that "bad guys" (black hat hackers) use for acquiring information is called social engineering.

One of the many definitions of social engineering is "social engineering is science, of skilfully manoeuvring human beings to take action in some aspect of their lives". [1] Another definition is that "social engineering is the act of tricking someone into divulging information or taking action, usually through technology". The idea behind social engineering is to take advantage of potential victim's natural tendencies and emotional reactions. [6]

We are witnessing the use of social engineering. The basic purpose of social engineering was in the style of "cheating people in order to get some information from them". Bad guys pretend that they are some third person (fake identity), and are trying to steal some confidential information, for example passwords, personal data, bank transactions, in every possible way, through direct interactions such as face-to-face interview or communication over the telephone, or indirect interaction through letters, emails and websites, or even unidirectional interaction, e.g. leaving an USB on the ground and wait for the target to pick it up. [4]

Social engineering attack is multifaceted and includes physical approach, social approach, reverse social engineering and technical approach. [2] Every approach is used in different stages of the actual attack. The basic purpose of social engineering attack is to avoid cyber security systems through deceit, exploiting the weakest link, and the people involved. [3] Some social engineering attack techniques used by the black hat hackers are: baiting, scareware, pretexting, phishing, spear phishing. [7]

There are a lot of classical examples of social engineering. In the game field, there are confidence games that were used in the 19th century where a person acquires another person's confidence by false pretences or false promises for a subsequent betrayal to obtain money or property from the victim [5]. Psychological manipulation, also known as propaganda, influenced many people in the Second World War to come out and buy military bonds. In the advertising field there is the sentence "You are not beautiful enough, if you do not buy that product".

Social engineering is using human psyche by utilizing powerful emotions such as fear, urgency, curiosity, compassion, or the strongest feelings of all of them: the desire for free things.

[1] ICT - Information and communication technologies

2. Acquiring information by using an image

Since information can be of a different nature, surely after reading the title, there is a question: "What type of information is it?". In this paper, we will explain a new technique of using social engineering to extract information that is difficult to extract. Concretely, we will present how to extract sensitive information by using an image that is posted on some social network. The success of this technique would be if we acquire the following information: the user's IP address, hostname, what web browser and operating system he/she uses, location / geographic coordinates, which ISP[2] it uses, city, state, country, and the date and time when that link is clicked (visited).

For successful use of this technique, we will need several distinctive components such as web programming, web hosting, domain, and, of course, a good idea and resourcefulness.

After we explain the distinctive components for using this technique, in the following section, step by step, we will explain the technique of acquiring information by using an image.

Step 1:

In this step we will need to create a small but smart tool for acquiring data using the PHP programming language. The code, which is only a part of this technique, is given in appendix A.

The main purpose of the PHP code is to acquire the following information: the user's IP address, hostname, what web browser and operating system he/she uses, location / geographic coordinates, which ISP it uses, city, state, country, and the date and time when that link is clicked (visited). From the PHP code, we can notice that all the information will be recorded in a file called "digitalforensic.csv". After recording the information in the file "digitalforensic.csv", the victim will be redirected on another web page. In this case, the victim will be redirected to the follow url: https://www.facebook.com/digitalforensic. This attack would be unnoticed if the victim had a high-speed Internet access.

When we finish programming, it is necessary to name this file. In our case, the file will be named "digitalforensic.php", and it will be attached to the hosting server. The file we attached to the following url: *http://www.digitalforensicx.com/digitalforensic.php*

Step 2:

Once we created the "digitalforensic.php" file, it is necessary to create one more file. This time we will create an html file named "digitalforensic.html". The code is given in appendix B.

This part of the code has two tasks. The first one will be to display the image that we have selected, i.e. to show the victim's image. The second one will be the victim to be redirected to the web address where the information will be acquired, i.e. to be redirected to the "digitalforensic.php" file. The file will be hosted on the following link: *http://www.digitalforensicx.com/digitalforensic.html*

Depending on the entered link in the "digitalforensic.html" file, an appropriate image (picture 1) will be displayed.

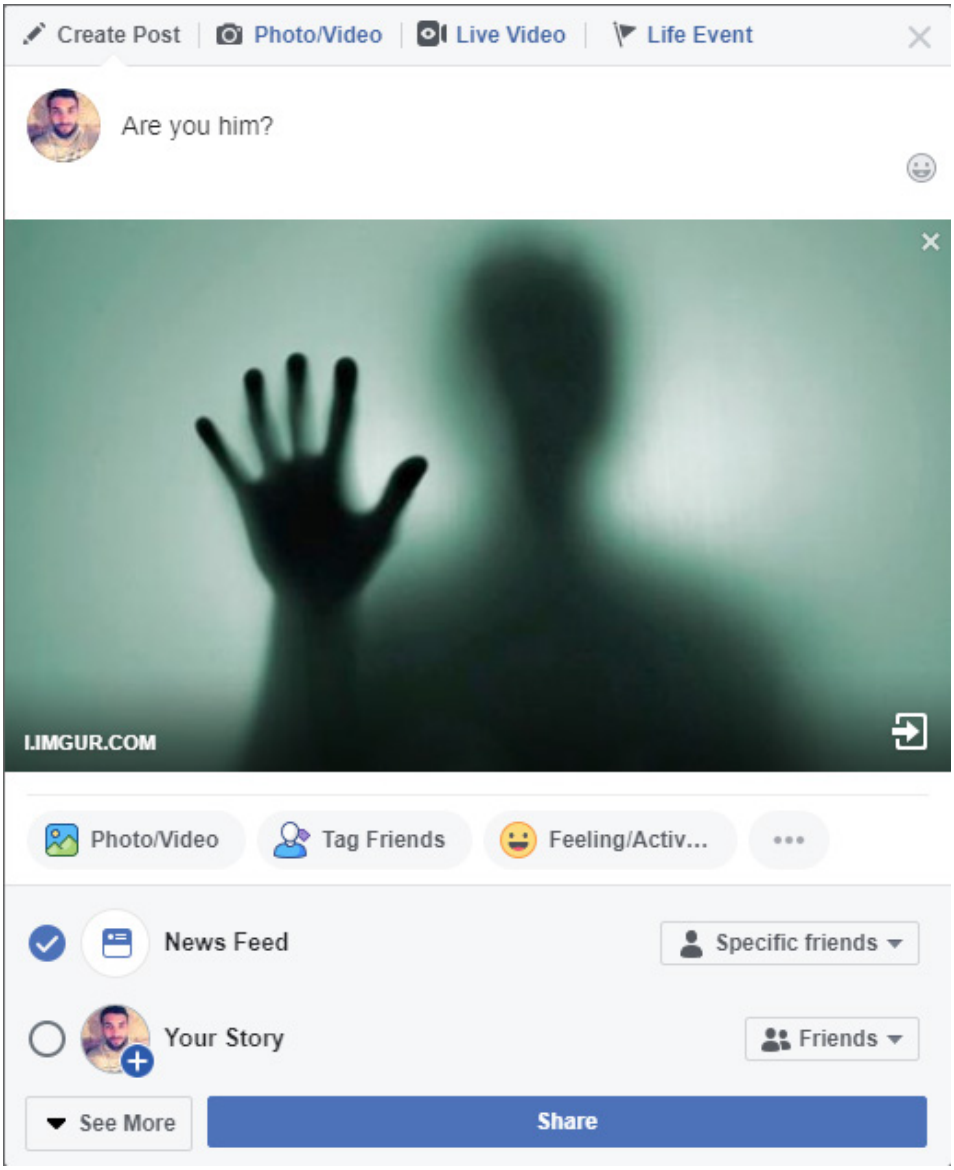
Picture 1: *Image of a victim*

[2] Internet service provider

Step 3:

This is the final step for the realization of the attack. In this step, we will need to choose where to launch the attack. In our case, we choose a social network called "Facebook" to launch the attack. To realize the attack, we should create a new post in which we need to insert the created html file called "digitalforensic.html", shown in step 2. Next, we will need to specify the target. That we will do in the "Specific friends" section with selecting the concrete target.

If we did everything correctly, we will get an image as shown on picture 2.



Picture 2: *Real view using this technique*

As a target we choose the person Mladen. We get a link to an image of that person and paste it in the file "digitalforensic.html". Then we copy the link from our hosted "digitalforensic.html" file and paste it on our Facebook profile, and then we get the image of Mladen.

If we want the attack to be more successful, we must display the image on Mladen's Facebook profile. For this we can use the same technique, but we need to insert the link on his Facebook profile instead of ours.

When Mladen signs in on Facebook, he will see the image of him (picture 3).

Picture 3: *Final view on Facebook*

Step 4:

The last step is to view the information. In this step, results will be displayed if user Mladen has seen the image and he will be redirected to the follow url: http://www.facebook.com/digitalforenic.

Now we can see our information on the url: http://digitalforensicx.com/digitalforensic.csv

93.53.53.92	ctel-92-53-53-92.cabletel.com.mk	Mozilla/5.0	41.0311,21.3403	AS43612 Company for	Skopje
92.53.53.92	ctel-92-53-53-92.cabletel.com.mk	Mozilla/5.0	61.0311,21.3403	AS43612 Company for	Bitola
92.53.43.47	ctel-92-53-53-47.cabletel.com.mk	Mozilla/5.0	81.0311,21.3403	AS43612 Company for	Prilep

Picture 4: *View of the information*

The information will be saved in a Microsoft excel document, because in step 1 we have declared it. In this document, we can see all the information we have coded in the PHP file. With some minimal changes in the PHP code, we will see different information in this document.

3. Conclusion

In this modern era, where everything is digitized, the use of the Internet increases. Because of that, today, social engineering is widely and actively used by black hat hackers for stealing sensitive information. Every day social engineering is increasing in sophistication and ruthless efficiency. Social engineering attack techniques used by black hat hackers are different depending on the goal. In this paper we describe a modern social engineering technique that can be used for acquiring information by using an image. This technique can be used on any social medium or web site. For the end, we believe that we open the eyes of people wide to be more cautious about where and which images they open on the Internet, because not every image is posted with a good purpose.

References:

[1] *Hadnagy, C.: Social engineering: The Art of Human Hacking*, Wiley Publishing, Inc., 2011
[2] Krombholz, K., Hobel, H., Huber, M., Weippl, E. : *Advanced Social Engineering Attacks*, SBA Research, Favoritenstraße 16, AT-1040 Vienna, Austria, 2014
[3] Breda F., Barbosa H., Morais T. : *SOCIAL ENGINEERING AND CYBER SECURITY*, Conference Paper, 2017, (downloaded from: https://www.researchgate.net/publication/315351300)
[4] Fan, W., Lwakatare, K., Rong, R. : *Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations*, I. J. Computer Network and Information Security, 2017, p. 4
[5] *Orbach, B., Huang, L.:* Con Men and Their Enablers: The Anatomy of Confidence Games, 85 Social Research 795, 2018, p. 810
[6] *Norton*: What is social engineering? Tips to help avoid becoming a victim, https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html
[7] *Imperva*: What is social engineering, https://www.imperva.com/learn/application-security/social-engineering-attack/

Mladen Kiprijanov
M.Sc of Computer Science in the field of Digital Forensics
Republic of North Macedonia
E-mail address: mladen.kiprijanov@outlook.com

Saso Gelev
University Goce Delcev- Stip Faculty of Electrical engineering
Krste Misirkov nmb 10-A, Stip
Republic of North Macedonia
E-mail address: sasogelev@gmail.com

Davor Vasilevski
Bureau for Development of Education
Rugjer Boshkovikj 20, Skopje
Republic of North Macedonia
E-mail address: davorvasilevski@bro.gov.mk

APPENDIX A

```
<?php
// Digital Forensic
// Mladen Kiprijanov.
// 08 Septembar, 2018.

// Name of the ip address log.
$outputWebBug = 'digitalforensic.csv';

function get_content($URL){
$ch = curl_init();
curl_setopt($ch, CURLOPT_RETURNTRANSFERR, 1); curl_setopt($ch, CURLOPT_URL,
$URL);
$data = curl_exec($ch); curl_close($ch);
return $data;
}

//Get the ip address and info about client.
$details = json_decode(get_content("http://ipinf/{$_SERVER['REMOTE_ADDR']}/json"),
false);
@ $hostname=gethostbyaddr($_SERVER['REMOTE_ADDR']);

// Get the query string from the URL.
$QUERY_STRING = preg_replace("%[^/a-zA-Z0-9@,_=]%", '',
$_SERVER['QUERY_STRINGG']);

// Write the ip address and info to file.
@ $fileHandle = fopen($outputWebBugg, "a"); if ($fileHandle)
{
$string ='"'.$QUERY_STRINGG.'","' // everything after "?" in the URL
.$_SERVER['REMOTE_ADDR'].'","' // ip address
.$hostname.'","' // hostname
.$_SERVER['HTTP_USER_AGENT'].'","' // browser and operating system

.$_SERVER['HTTP_REFERER'].'","' // where they got the link for this page
.$details->loc.'","' // latitude, longitude
.$details->org.'","' // internet service provider
.$details->city.'","'                    // city
.$details->region.'","' // state
.$details->country.'","' // country
.date("D dS M,Y h:i a")."' // date
."\n";
$write = fputs($fileHandle, $string);
@ fclose($fileHandle);
}
header('Location: https://www.facebook.com/digitalforensic');//RedirectURl

echo '<!DOCTYPE html><html><head><title>DF Tools</title></head><body>'; echo '</
body></html>';
?>
```

APPENDIX B

```
<html prefix=”og: http://ogp.me/ns#”>
    <head>
    //Link to the victim’s image
    <meta property=”og:url”  conent=”https://i.ytimg.com/vi/_LU_J0PTgbs/maxresdefault.jpg” />

    <scrip type=”text/javascript”>window.location =
“http://digialforensicx.com/digitalforensic.php”;</scrip>
    </head>
    </html>
```