Journal of Novel Applied Sciences
Available online at www.jnasci.org
©2016 JNAS Journal-2016-5-9/402-407
ISSN 2322-5149 ©2016 JNAS

Design a new and innovative framework to deal with phishing websites based on random networks

Saeed Teimoori

Faculty of Mathematical science, university of Mohaghegh Ardabil, , Ardabil, Iran

Corresponding author: Saeed Teimoori

ABSTRACT: Phishing websites are fraudulent webpages by people with grudging is created to imitate real websites and legal. Many of these types of webpages with high visual similarities are the tricks of the victims. Victims of phishing websites are possible that bank account, password, credit card numbers and other important information puts at the disposal of owners and phishing websites designers. Increasingly phishing websites has become to a big challenge in the field of e-commerce and especially e-banking. In this paper a new and innovative framework is provided to deal with phishing websites based on random network. Using the technique of random networks, the security image turns into two different random networks. Each of random networks alone does not give at the disposal of user information from the security image. Only when both random networks are available, the security image is reconstructed to the initial state.

Keywords: Phishing websites, Random networks, Cryptography, Security image.

INTRODUCTION

Phishing websites is unaware method to creating a copy of legal webpages to users which its purpose is to obtain personal information and financial data from users (Malware 2006) [1]. Phishing is including scams websites online that has the potential both for victims, organizations and financial institutions involves costs after the development of online financial services and e-commerce, phishing websites attacks has become to one of the dangerous and widespread attacks on internet platform. Research has shown that phishing webpages are growing at a rapid rate in recent years. The most important harmful effects of phishing websites are creating a crisis of confidence. Trust is one important factor in the success of e-commerce and e-banking.

To deal with phishing websites are provided so far diverse and various of methods. One of the most popular and most used methods deal with phishing attacks is using from phishing filter in Internet browsers. Phishing filter acts based on a blacklist of websites that have been identified as phishing. In other words, phishing filter prevents from user activity on sites that have been identified as phishing. But the major problem is using of phishing filter in Internet browser that browser not have ability to identify new threats and new phishing websites that are not available in the database

Another widely used method it in various investigations in order to identify phishing websites is being used, the use of classification techniques is in data mining. For instance, in 2011, Chang and his colleagues are presented a general framework by using Bayesian method to detect and identify phishing websites based on content (Zhang, Liu et al., 2011) . In model proposed by Chang, by using of content textual and visual were investigated similarities between phishing websites and legal websites and to obtain specific criteria, was performed classification action. Also, Chen and his colleagues were provided other method based on a data mining for assessing the severity of phishing attacks in 2011(Chen, Bose, .et al, 2011). In the proposed method was evaluated the intensity of phishing attacks in target organizations with descriptions dangerous levels. The main problem use of classification techniques in data mining to detect phishing websites is the error rate in these hands of methods. In fact, these methods are unable to detect all phishing websites.

The use of cryptography security images is another method in much of the research is being used to detect phishing websites. Some of these methods can be cited to method presented by Frida in 2013(Freeda and Sindhuja, 2013). In the method presented by Frida, security image in a legitimate website, coded by visually cryptography techniques and using images obtained encrypted, the user is able to recognize similar phishing websites. This paper is organized in five sections. In continuation will be discussed and in the second section are introduced random networks and types of algorithms. The proposed framework will be explained in the third section and results of the implementation in fourth section. Finally and in the fifth section will be explained conclusions.

2. Random networks

Random network and as well as cryptography of digital images were introduced by random network first time by Kafri and Keren (Kafri and Keren, 1987). A random network is a two-dimensional array of pixels. Each pixel in a random network is completely transparent or opaque and determine transparent or opaque pixels of a random network is done in a completely random process, so there is not any correlation between the values of different pixels in the array. In a random network zero represents transparency and one indicates being opaque. Considering that probability of being transparent or opaque pixels of random network is equal, as a result, the average degree of brightness in a random network will be equal to 1/2. Suppose a random network and then the average degree of brightness of this random network is shown in Equation 1.

$$T(R)=1/2 \qquad (1)$$

Keren and Kafri provided three different algorithms based on random networks for cryptography binary images. The proposed cryptographic algorithms R_1 and R_2 produces two random network that each of them alone may disclose binary image data is not encrypted. While if they are matched on each other, causing detection of desired image. In order to obtain the decrypted image, two random networks by using of operator OR on each other. One algorithm introduced by Kafri and Keren, will be presented. In the presented algorithm $\overline{R}$ is represents a random network complement R . As well as function $Random-pixel\,(0,1)$ randomly generates values zero and one.

Algorithm 1

```
1.   Generate $R_1$ as Random Grid, $T(R_1)=1/2$
     //for (each pixel $R_1[i,j]$, $1 \le i \le w$, $1 \le j \le h$) do
     //      $R_1[i,j]$=random_pixel(0,1)
2.   for (each pixel B[i,j], $1 \le i \le w$, $1 \le j \le h$) do
2.1  {      if (B[i,j]=0)  $R_2[i,j]=R_1[i,j]$
            else $R_2[i,j]=\overline{R_1[i,j]}$
     }
3.   output ($R_1$,$R_2$)
```

Algorithm 2

```
1.   Generate $R_1$ as Random Grid, $T(R_1)=1/2$
     for (each pixel B[i,j], $1 \le i \le w$, $1 \le j \le h$) do
2    {      if (B[i,j]=0)  $R_2[i,j]=R_1[i,j]$
            else $R_2[i,j]$=random_pixel(0,1)
     }
3.   output ($R_1$,$R_2$)
```

Algorithm 3

```
1.  Generate $R_1$ as Random Grid, $T(R_1)=\frac{1}{2}$
      for (each pixel $B[i,j]$, $1 \le i \le w$, $1 \le j \le h$) do
2   {     if ($B[i,j]=0$)  $R_2[i,j]$=random_pixel(0,1)
          else $R_2[i,j]=\overline{R_1[i,j]}$
      }
3.  output ($R_1$,$R_2$)
```

Images obtained by decryption process in the algorithm Keren and Kafri were not appropriate for visual quality. For this reason, Kumar and Sharma in 2012 in order to raise visual quality of decoded images, done to improve Keren and Kafri algorithms (Kumar and Sharma, 2012). In method proposed by Kumar and Sharma, the encryption process is exactly the same the encryption process Kafri and Keren but instead of using operator OR in the decoding process used from operator XOR .

3. The proposed framework

In this section, in order to recognize and identify phishing Web sites, a new and innovative framework will be presented based on random networks. The framework presented in this section, to deal with phishing websites, from security images have benefited. In order to use the security images to prevent phishing attacks is used in the proposed framework of random network techniques. The proposed framework consists of two main phases of registration and verification. Then will be introduced each of phases mentioned.

3-1. Registration phase

In registration phase are requested a key of user by legitimate and valid web site. Key received from the user with a random key generated by legal website server combined and produces the security image (Aravind and Krishnan, 2014). The security image obtained by using an encrypted algorithm numbers one and generated two random networks. First random network and security image are generated and taken in disposal of user in the verification phase. Also, the second random network and security image is storing in the database valid website server. In addition to storing data in the database, to each user a unique ID number will be assigned. Registration phase is shown in the Figure 1.

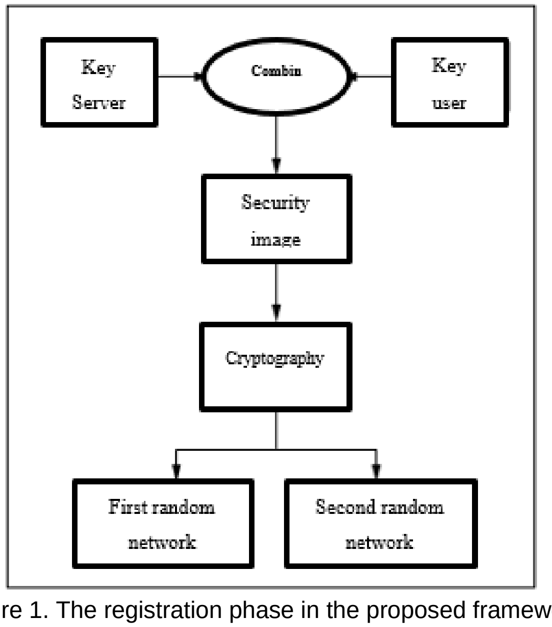

Figure 1. The registration phase in the proposed framework

3-2. Verification Phase

In the verification phase, the user wants to log into the website. In this phase, in first user will be asked to enter own ID number. Then, in order to login to the website, the user must enter own random network. Random network entered by the user, transfers to the server that is stored the second random network. Two random networks by using operator XOR decoded and the security image is produced. The security image produced is shown to the end user and the user by comparing the displayed image and the security image that were given in the time of registration, can recognize validity of the website. If the website was valid, the user by using security key contained in security image at its disposal can easily enter the website. Figure 2 shows verification phase in the proposed framework to deal with phishing attacks available on the web site.

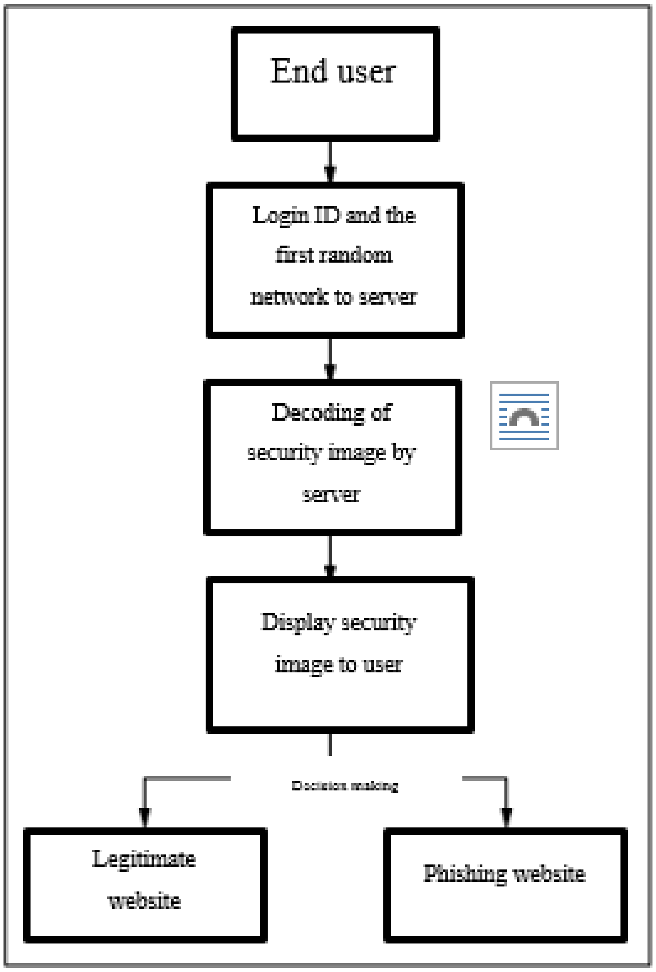
End user
Login ID and the first random network to server
Decoding of security image by server
Display security image to user
Decision making
Legitimate website
Phishing website

Figure 2. Verification phase in the proposed framework

4. The implementation of the proposed framework

In this section the results of implementing the proposed framework to deal with phishing website will be provided. As stated in section III, in the registration phase security image encrypted by the algorithm number one and the result of this process will be generated the two random networks. The first random network and security image is providing at the disposal of user and the second random network storing server in the valid website. Finally, in verification phase by using two networks random will be regenerated initial security image. Figures number three and four shows respectively registration and verification phase in the proposed framework.

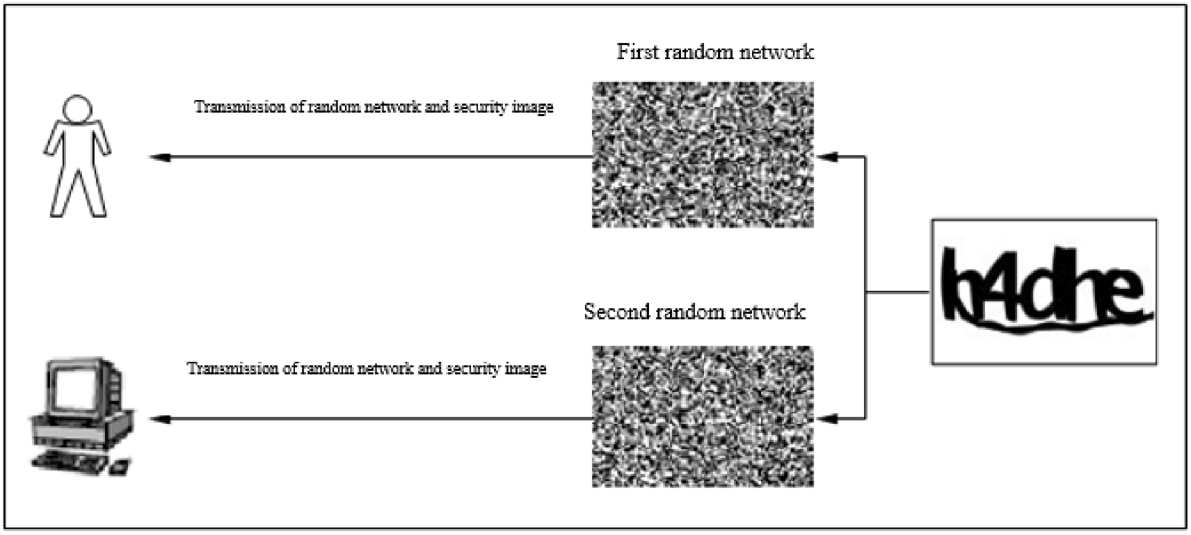
First random network
Transmission of random network and security image
Second random network
Transmission of random network and security image
h4dhe

Figure 3. The implementation of registration phase in the proposed framework

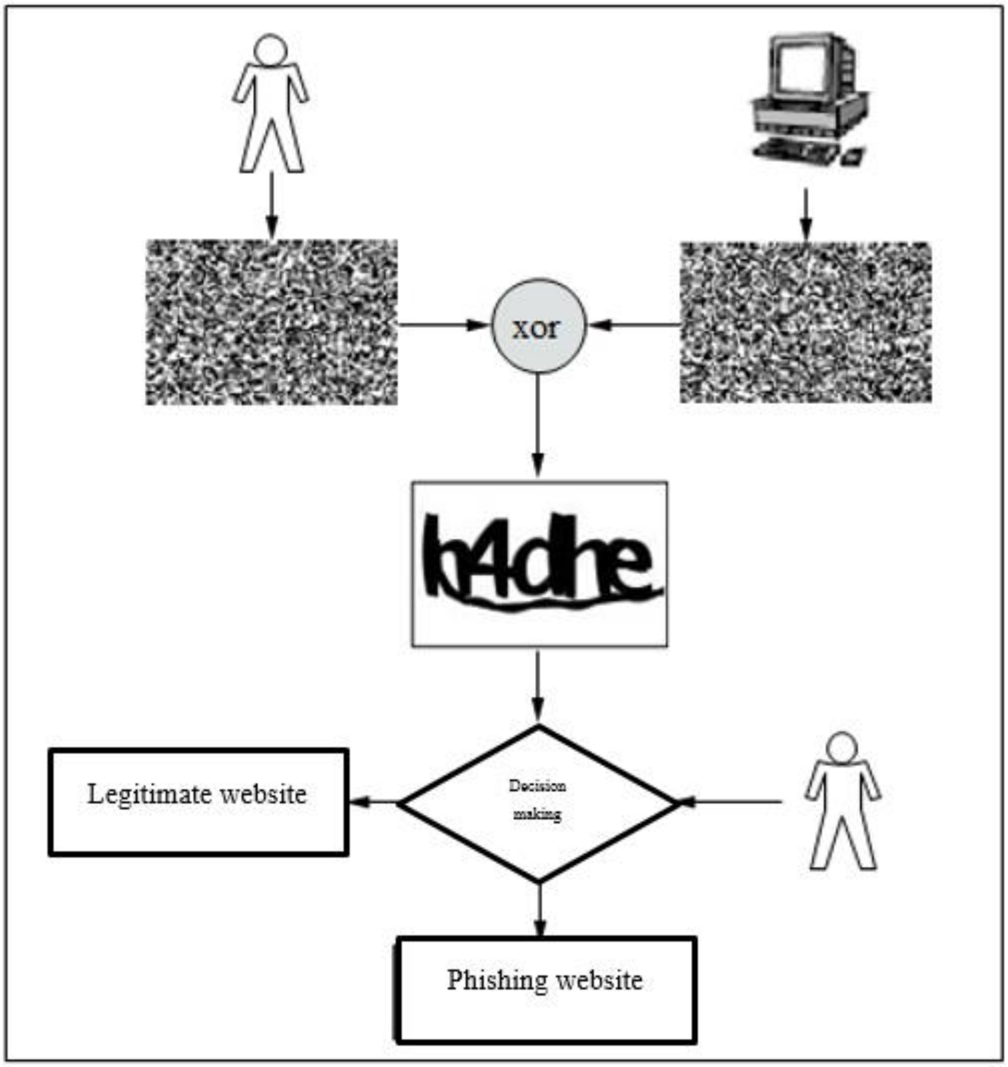

Figure 4. The implementation of verification phase in the proposed framework

According to the results obtained of implementing the proposed framework, it is clear that phishing website in any way not have the ability to reconstruct security image and random networks. Due to the inability on restructure random networks that each of random network is generated in the process completely random which is impossible practically reconstruction a random network.

CONCLUSION

Scope and complexity of phishing websites are rapidly increasing so that in recent years has become a low-cost non-professional activities to an organized crime the Internet. A Websites phishing attack has not only negative effects on corporate earnings and financial organizations but also makes non-confidence users of e-commerce and electronic banking. Therefore deal with such websites in cyberspace is very necessary and important. In this research provided a new framework to deal with phishing websites that is based on image cryptography security on random networks. The framework is presented in such a way that the legality of a website is only detectable by the user.

REFERENCES

Aravind K.A and Krishnan R.M.V. 2014. Anti-phishing frame work for banking based on visual cryptography. International journal of computer science and mobile applications, 2 (1): 121-126.

Chen X, Bose I, Leung A.C.M.L, and Guo C. (2011). Assessing the severity of phishing attacks: a hybrid data mining approach. Decision support system, 50: 662-672. Freeda A, Sindhuja M, and Sujitha K. 2013. Image captcha based authentication using visual cryptography. International journal of research in engineering & advanced technology, 1(2): 1-6.

kafri O and keren E. 1987.encryption of pictures and shapes by random Grids. Optics Letters, 12(6): 377-379.

Kumar S. and Sharma R.K.2012. Improving contrast in random grids based visual secret sharing. International journal of security and its applications, 6 (1): 9-27.

Malware M .2006 .Anti-Phishing Best Practices for ISPs and Mailbox Providers, 2(1): 1-6.

Zhang H, Liu G, Chow T.W.S, and Liu, W. 2011.Textual and visual content-based anti-phishing a Bayesian approach. IEEE transactions on neural networks, 22(10): 1532-1546.