

Dynamic Watermarking for Prevention Phishing Attack

By

Manoj Kumar Pandey ,Rakhi Singh, Gagan Tiwari

Deptt. Of MCA-GCET, Greater Noida, UP, INDIA

manojglaitm@gmail.com, rakhi2k11@gmail.com , tiwari.gagan@gmail.com

ABSTRACT

According to this approach user will be asked for some additional information like watermark image, its fixing position and secret key at the time of user's registration and these credentials of particular user will be changed at per login. During each login phase a user will verify the authentic watermark with its position and decide the legitimacy of website.

Nowadays phishing attacks are increasing with burgeoning rate which is highly problematic for social and financial websites. Many anti-phishing mechanisms currently focused to verify whether a web site is genuine or not. This paper proposes a novel anti-phishing approach based on Dynamic watermarking technique.

Keywords

Phishing Attack, Watermarking, Website, Authentication

1. INTRODUCTION

This attack treated as a deceptive phishing attack which target to the financial organization. Criminals complete their life cycle in very short period by the login and personal detail of the people. Phishing attack has various types as deceptive, malware, key loggers, data theft, search engine, content injection and web trojan. Many anti phishing tools exist to protect the attack. Juan Chen et.al .have proposed a very standard approach in [1].

Today all organizations are using the internet for sharing the message so the communication must be secure. Few unethical hackers are doing the cyber criminal activity by committing fraud. Attacker sends the phishing message by the fake website that looks like a original site. According to their idea they have propose a new end-host based anti-phishing algorithm, which is called Link Guard, which works by utilizing the generic characteristics of the hyperlinks in phishing attacks. These characteristics are derived by analyzing the phishing data archive provided by the Anti-Phishing Working Group (APWG). Because it is based on the generic characteristics of phishing attacks, Link Guard can detect not only known but also unknown phishing attacks. Michael Atighet-chi et .al. have given the idea in [2]. They suggested a framework based on attribute based checks for defending against phishing attacks. According to Amir Herzberg et.al.s approach presented in [3] they present an improved security and identification indicators, as author implemented, a browser extension in Trust Bar. Dmytro Iliev et.al.s proposed idea in [7] phishing prevention approach based on mutual authentication is provided. Mohsen Sharifi et.al. have

suggest an idea in [4] AntiPhishing Authentication (APA) technique to detect and prevent real-time phishing attacks. Daisuke Miyamoto et.al.s gave an approach in [5] on performance of machine learning-based methods such as Regression Trees and Classification, Naive Bays, Additive Regression Trees , Logistic Regression for detection of phishing sites. Daisuke Miyamoto et.al. Proposed approach in [6] that is study of users past trust decisions (PTDs) for improving the accuracy of detecting phishing sites. Mercan Topkara et.al. have suggested an approach using watermark in [8] which is called ViWiD. ViWiD is an integrity check system based on visible watermarking of logo images. Various webpage related security using watermarking technique is discussed in [9][10][11][13][14]. Section 2 describes the proposed algorithm. Section 3 contains all experimental results and section 4 concludes the paper.

2. PROPOSED ALGORITHM

There are many methods proposed earlier to detect and prevent phishing attack. Some of them use watermark technique and some them uses another approach. There is some limitation in this approach like many checks and enforcements which are used by the client-side defense tools can be tricked by attackers after getting a reasonable knowing of web site construction [4]. For example, using mosaic attack, an attacker can make fool the image check system of Spoof Gaurd by partitioning the logo image into small parts and show it in such way that it looks like legitimate one. Some time due to irritation of some protection means like antivirus, user turnoff the protection mechanism of client side. Hence all client side schemes will live all defensive actions. Similarly in case of tools which are based on cryptography, they need individual downloaded software in each client side machine. In some cases in spite of using SSL secure connection, if client authentication tool will be turned off, it may suffers with Phishing attack. Few earlier proposed algorithms also use watermarking technique but visible and stationary nature of their watermark may also suffer with phishing attack. In this paper we are proposing an approach for prevention of phishing attack based on dynamic position watermarking technique. This approach is divided in to three modules viz. Registration process, Login verification process and Web site closing process. Different position for watermark image can be top left, bottom left, top right, bottom right, center.

2.1 Registration process

This is the initial phase whenever we open the website and trying to become a member of the website. Hence first communication between client and server is done in this phase. Most of the financial, social networking web site gives the opportunity to make an account in their server by uploading user credentials like user name and password etc. These credentials play vital role for further communication with those web site. There are three phase in registration process. You have more than one assuming, please make sure that the Volume Editor knows how you are to be listed in the author index.

Step 1- Client will open the web page which starts with registration phase. There will be five most essential credentials of user viz. Username, Password, Secret key, Watermark Image and position of watermark. Here Secret key will be unique for each user and hence it is called primary key. Since we are assuming a secure channel between client and server, hence all credentials will be in encrypted form and there will be no attacks like man in the middle.

Step 2- In this phase web site hosting server will store all data related to particular user. Here Secret key will be primary key for the database.

Step 3- User is acknowledged with a proper web page having desired watermark at predefined location. Now the user will get login page for entering his username and password.

2.2 Login Verification Phase

This is the very critical phase which mostly suffers with phishing attack because most of the attackers create a fake website similar to the legitimate one. This phase consist of eight steps.

Once user has created his account he needs to log in the web site Step 1- whenever user will open the website he will be asked for proper Secret key which is unique for each user. In this phase there will not be login window.

Step 2- A query will be forwarded to database of server for retrieving all credentials of user associated with that particular secret key.

Step 3- After getting a proper match from database, two important credentials (Watermark image and its position) will be returned to website hosting server.

Step 4- Login page will be displayed to user with proper watermark image and its location as set by user at the time of registration.

Step 5- After ensuring the correctness of watermark image and its position, a legitimate user will verify the authenticity of the website and then only he will enter his login id and password.

Step 6- A query will be passed to database for entered username and password.

Step 7- Now according to username and password, all information related to that particular user will be retrieved from database to the server.

Step 8- A proper account will be shown to user which is of legitimate website. Now we can trust on that website.

2.3 Website Closing Phase

Proposed algorithm is based on dynamic watermarking, hence at per login the position and nature of watermark must be changed which is only known to legitimate user.

Step 1- User starts the closing process by clicking on the close button.

Step 2- During logout, user will be prompt for reentering the new watermark image and its location. This step is very essential and cannot be ignored.

Step 3- After resetting the watermark image and position, user must have to wait for acknowledgment from server.

Step 4- These all new information will be stored in database and old information will be invalidated.

Step 5- After successful updating user will be acknowledged.

2.4 Determination of Phishing Website

As soon as user will click on suspicious link, fake website will be open which is ask for secret key.

Suppose attacker has created a phishing website which looks similar to the original one. Step 1- In this step user will enter the secret key and wait for the desired watermark image at particular position.

Step 2- A fake website will not have the database related to watermark information and its position. That's why it will be very difficult to determine or guess the correct watermark and position by attacker.

Step 3- Due to absence of proper watermark and its location user can determine that it is not authorized one and he is going to be suffered with phishing attack.

In this case the user must open the proper website by verifying the URL and then must change his current secret key by newer one. Because attackers now aware with the old secret key. Hence we will invalidate that secret key. When user enters correct username and password, then only he can see his account of website, so here our main aim is to protect username and password. Suppose if an attacker knows the secret key, which is not changed by newer one till now. At that condition the watermark image and its position doesn't matter for the attacker. Now he will get login page but still unaware of username and password so he will not be able to see the account information as well as he cannot change the secret key because during changing it, a attacker must know all credentials of user.

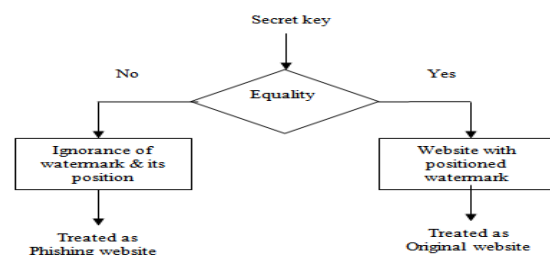


Fig 1. Decision of website is phishing one or original one

Hence the flowchart given in figure 1 will demonstrate the procedure to determine whether the website is phishing one or original one.

3. EXPERIMENTAL RESULTS

Proposed algorithm is implemented and verified over the Local area network. First of all users has created his account and stored his credentials over the server database. Here we have taken a passport size photograph as a visible watermark and chosen the top left position as a location for watermark. In our experiment we have created a website for a bank named ABC Bank. After creating an account whenever we open the web site it will be looked like figure and it will only prompt for secret key as set by legitimate user at the time of registration. Once we have entered correct secret key it will show the web page look like



Figure 2. by which a user can verify the watermark and its location and according to this information he can assure that opened website is authentic one.



Fig.3. Web page for login and password insertion
Now the user will be prompted for username and password. After entering correct user name and password user will able to see his actual account information from a legitimate and desired website. This is the exact way to prevent from Phishing attack as proposed in this paper.

4. CONCLUSION

In this paper, we propose a new anti-phishing approach based on Dynamic watermarking technique. Watermarking third party, nor requires any plug in or online tool hence

this approach is more user friendly than the previous approaches. Experimental results show the working of our approach in which a user requires only different watermark at the time of per login which is more tolerable than being hacked by attacker. It is clearly revealed that by determining the main differences between the legitimate website and the phishing, one can reduce the risk of this type of attack. According to experimental results it is clear that proposed approach is more applicable for social and financial websites than others.

5. REFERENCES

- [1] Mohsen Sharif, Alireza Saberi, Mojtaba Vahidi, and Mohammad Zorufi, A Zero Knowledge Password Proof Mutual Authentication Technique against Real-Time Phishing Attacks, Springer-Verlag Berli Heidelberg 2007.
- [2] Daisuke Miyamoto, Hiroaki Hazeyama and Youki Kadobayashi, An Evaluation of Machine Learning-Based Methods for Detection of Phishing Site, Springer-Verlag Berlin Heidelberg , 2009.
- [3] Daisuke Miyamoto, Hiroaki Hazeyama and Youki Kadobayashi, Human Boost: Utilization of Users past Trust Decision for Identifying Fraudulent Websites Springer Verlag Berlin Heidelberg, 2009.
- [4] Dmytro Iliev, Yong Bin Sun, Website forgery prevention IEEE 2010.
- [5] Mercan Topkara, Ashish Kamra, Mikhail J. Atallah and Cristina Nita Rotaru, ViWiD: Visible Watermarking Based Defense Against Phishing, Springer-Verlag Berlin Heidelberg, 2005.
- [6] Franco Frattolillo, Watermarking Protocol for Web Context, IEEE Transactions on Information forensics and security, vol.2, no.3, sept , 2009.
- [7] Cong Jin, Hongfeng Xu, Xiaoliang Zhang, Web Pages Tamper-Proof Method Using Virus-Based Watermarking, . IEEE, 2008.
- [8] Juan Chen and Chuanxiong Guo, Online Detection and Prevention of Phishing Attacks, IEEE, 2006.
- [9] Michael Atighetchi and Partha Pal., Attribute-based Prevention of Phishing Attacks, IEEE Int. Symposium on Network Computing and Applications, 2009.
- [10] Amir Herzberg, Ahamad Jbara, Security and Identification dicators for Browsers against Spoofing and Phishing Attacks, ACM Mohsen Sharif, , A Zero Knowledge Password Proof Mutual Authentication Technique Against Real-Time Phishing Attacks, Springer-Verlag Berli Heidelberg , 2007.
- [11] Mitsuo Okada, Yasuo Okabe and Tetsutaro Uehara, A Web-based Privacy-Secure Content Trading System for Small Content Providers Using Semi-Blind Digital Watermarking, IEEE Communications Society subject matter experts for publication in the IEEE CCNC 2010.
- [12] Peng Sun, Hongtao Lu An efficient web page watermarking scheme, IEEE, 2009.
- [13] Peng Sun, Hongtao Lu, Two efficient fragile web page watermarking schemes Fifth International Conference on Information Assurance and Security, 2009.
- [14] Xianzhong Long, Hong Peng and Changle Zhang , A Fragile Watermarking Scheme Based On SVD for Web Pages, IEE, 2009