ANTI-PHISHING USING CAPTCHA

Aakash Badiyani
abadiyani@cllutheran.edu
California Lutheran University

Jaikit Jilka
jjilka@callutheran.edu
California Lutheran University

Jeet Kapadia
kapadia@callutheran.edu
California Lutheran University

ABSTRACT

Today life has become fast and everything work on the web. Internet has become essential for human development but with this era has emerged a new threat. As it is said “With great power comes great responsibility”. This new threat is called “Phishing”. A user’s data is very sensitive and confidential and poses a threat if it is leaked. As nowadays a lot of information sharing happens over the network it is important to safeguard a user’s confidential data. In phishing an attacker impersonates a trustworthy organization and gets hands on a user’s private data such as username or id, password and bank-account details. Other sensitive data like contact information, age, race, address can also be exposed. This makes the user and the original organization both vulnerable to this kind of attack. To counter this attacks there are many solutions out of which one can be use an image CAPTCHA for authentication. This uses visual cryptography for safeguarding vital and important information. Prior to registration an original CAPTCHA is shared with the user. This CAPTCHA is broken into two parts and one part is shared with the user while the other part is shared with the server. Both comply to this policy and together mitigate phishing.

INTRODUCTION:

Phishing has become one of the major issues in the recent times that have sent across an alarm for the internet users. The major reason for concern is the fact that phishing activity directly hits at us as it aims at securing our personal and sensitive information. In phishing, electronic mails or other form of communications are sent across to a specific targeted group of people asking for their credit card information, account details, usernames and passwords. These mails generally look very professional and bear the looks of official ones. It is one of the most disturbing problems that these sites make use of large entities names. Very often they give us the lure of large jackpots or job offers. All of these types of mails asking for personal and significant information are fake ones and are not to be believed. Thus we end up giving our confidential information to these web sites. Hence we need to device a mechanism that would test the website for its genuineness and also ensure the candid nature of the user.

BASIC CONCEPT

Here the user of a particular website needs to confirm that he/she is dealing with the right web site. For this the web site's authenticity should be checked and the user should gain the confidence accordingly. Once the website is known to be legitimate, the user can present his/her confidential information to it, being assured of his/her privacy. In case the website fails to prove its authenticity, the user would get cautious well in advance and refrain from giving any information to that particular site. Anti-Phishing threat needs to be eradicated and addressed using various techniques. This project has developed one such technique that can curb the threat of anti-phishing by the use of CAPTCHA which can provide us an improved effectiveness of the existing anti-phishing techniques. This project uses CAPTCHA in the authentication process and in addition to it during the registration phase as well as during the login phase. There is input provided by the server side during login phase to show its authenticity. Thus it is a highly complicated task for the phisher eventually reducing the phishing attacks.

AIMS AND OBJECTIVE:

Aim: This project aims at providing a mechanism on which a user could rely, gaining complete assurance of the privacy and various other aspects involved in a transaction over the internet. The chief goal in this project is to curb the most prevalent attack over the network, 'The Phishing attack' and to provide the most sought after security mechanism 'The Anti-Phishing technique'.

Objectives: To conduct any transaction on the internet in a secure manner, preventing phishing. To provide a way by which the user first makes sure that the website being dealt with is the actual one (i.e. to authenticate a web page). To prevent the user from access to a phished web page. To grant access to a legitimate page. The Objective of the project is to provide security to the user to safeguard its crucial credentials. It is done using CAPTCHA authentication technique. When the user first registers he/she is allotted a CAPTCHA share which is used during the login phase and during the login phase the user is first asked for its share and server share is provided by the server which can help the user to understand the authenticity of the server and then give is crucial password credentials. Thus the main objective stands out as providing an anti-phishing framework by implementing CAPTCHA authentication technique. Providing confidence to the user for the websites it is dealing with and thus encouraging him to conduct E-Commerce activities in a secure manner.

LIMITATIONS OF EXISTING SYSTEM

Detect and Block the Phishing Web Sites in Time

For DNS scanning, it increases the overhead of the DNS systems and may cause problem. For normal DNS queries, and furthermore, many phishing attacks simply do not require a DNS name. For phishing download detection, clever phishers may easily write tools which can mimic the behaviour of human beings to defeat the detection.

Enhance the Security of the Web Sites

With these methods, the phishers cannot accomplish their tasks even after they have gotten part of the victims' information. However, all these techniques need additional hardware to realize the authentication between the users and the Web sites hence will increase the cost and bring certain inconvenience. Therefore, it still needs time for these techniques to be widely adopted. Anti-Phishing Framework using Image CAPTCHA based Authentication

Block the Phishing E-Mails by Various Spam Filters Spam filters are designed for general spam e-mails and may not be very suitable for filtering phishing e-mails since they generally do not consider the specific characteristics of phishing attacks.

Install Online Anti-Phishing Software in User's Computers It is easy to observe that all the above defence methods are useful and complementary to each other, but none of them are perfect at the current stage.

PROBLEM STATEMENT

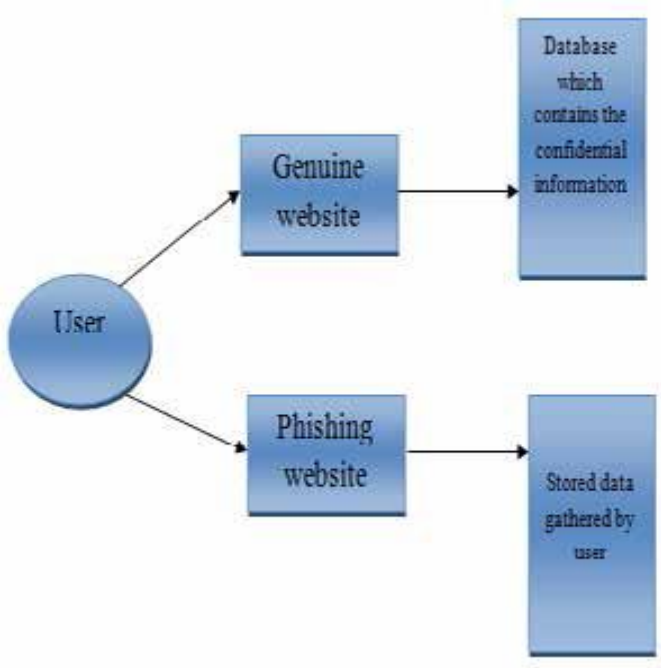
To control the phishing attacks, there should be a guarantee of the genuineness of the source requesting the information. Hence the primary issue is to verify the correctness of the source. For this purpose, this project employs the “Image CAPTCHA Authentication Based Visual Cryptography” in which a CAPTCA image will be split into 2 shares, 1 for each side (user and website) during the registration phase. In future when the user logs in to the site, the shares will be used to recompose the original CAPTCHA, which could be verified by the user, guaranteeing the authenticity of the source. Thus a robust, effective and latest algorithm is needed for generating CAPTCHA image as the older ones may not solve the purpose. The methods in the existing system are complicated for people but, on the other hand, they are easier for bots.

SCOPE

The number of conventional phishing attacks reported to the group rose from 14,987 in May to 15,050 in June. Meanwhile, the number of unique crimeware dedicated to password stealing doubled from 79 to 154 in the same period. These are some of the many facts that suffice to imply that the phishing attacks are prevalent all over the internet raising the risk of frauds done to all kinds of users ranging from laymen working with their bank accounts to the corporate people who deal with large amount of confidential information and financial transactions. This raises an alarm to both the sides of transaction, as the users would have their privacy and integrity as their outmost concern and the reputed organizations over the internet would always want to maintain their good will within their customers. Thus this project has a limitless scope in businesses of all domains active on the internet. With exponential increase in the deals over the net, 'Anti-phishing' mechanism is a security feature in high demand. It has its scope in the fields of e-commerce, e-banking and all such fields where monetary aspects and information transfer is involved. With further enhancement of this project from the commercial point of view, it will be market ready gaining customer confidence all over.

PROPOSED SYSTEM

For phishing detection and prevention, we are proposing a new methodology to detect the phishing website. Our methodology is based on Image Captcha Authentication Based on Visual cryptography scheme using visual cryptography. It prevents password and other confidential information from the phishing websites.



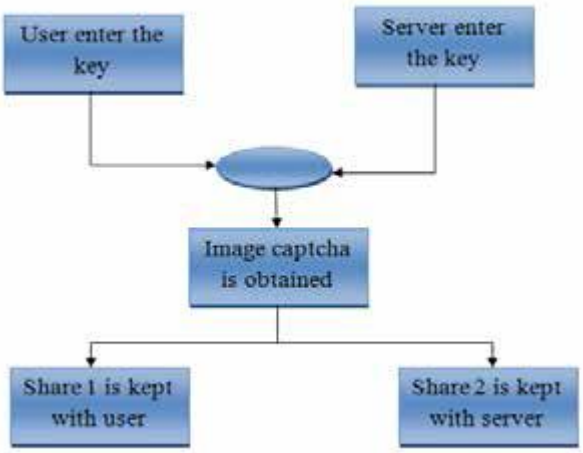
Current scenario

The proposed approach can be divided into two phases:

- Registration Phase
- Login Phase

Registration Phase

In the registration phase, a key string (password) is asked from the user at the time of registration for the secure website. The key string can be a combination of alphabets and numbers to provide more secure environment. This string is concatenated with randomly generated string in the server and an image captcha is generated.



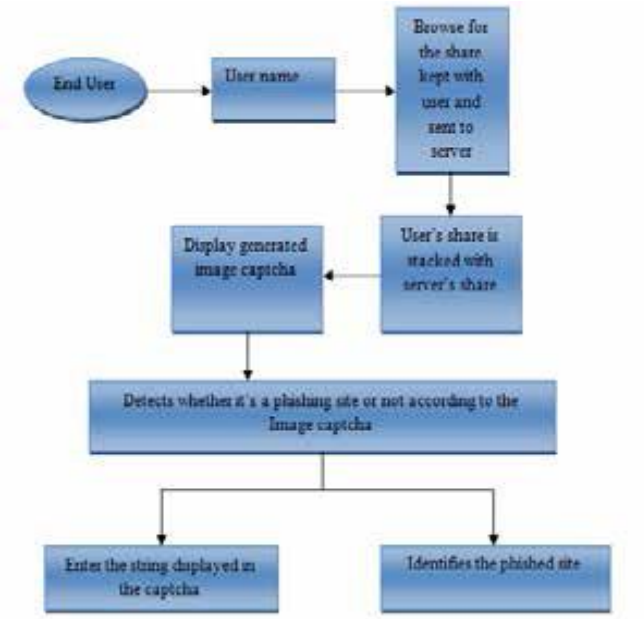
User registration process for the website

The image captcha is divided into two shares such that one of the shares is kept with the user and the other share is kept in the server. The user's share and the original image captcha are sent to the user for later verification during login phase. The image captcha is also stored in the actual

database of any confidential website as confidential data. After the registration, the user can change the key string when it is needed.

Login Phase

When the user logs in by entering his confidential information for using his account, then first the user is asked to enter his username (user id).Then the user is asked to enter his share which is kept with him. This share is sent to the server where the user's share and share which is stored in the database of the website for each user, is stacked together to produce the image captcha. The image captcha is displayed to the user. Here the end user can check whether the displayed image captcha matches with the captcha created at the time of registration. The end user is required to enter the text displayed in the image captcha and this can serve the purpose of password and using this, the user can log in into the website. Using the username and image captcha generated by stacking two shares one can verify whether the website is genuine/secure website or a phishing website and can also verify whether the user is a human user or not.



User Login for Website

RESULT:

The user needs to register himself/herself onto the website with all the necessary personal information. The user will have to take a note of the CAPTCHA presented at the bottom of the registration page. The registration phase starts with this webpage. The user will be sent an e-mail and an SMS confirming his/her registration. So now when the user logs in into the account he must get some random CAPTCHA on every stroke of a key in the CAPTCHA share space. However when the user types the correct CAPTCHA share, he/she must get the entire CAPTCHA correctly. When the user completes typing his/her share of the CAPTCHA the entire original CAPTCHA emerges. However if the correct CAPTCHA is not produced, the user must at once get alert and should hence refrain from giving any further information to that site. So if this mechanism is not present on the website there is a complete chance that the attackers will get the user id and the password as people can be easily bluffed by a fake URL. It appears that the implementation of the project is in complete accordance with the goal that was set before the commencement of the project. The intelligent phishers constantly update their techniques and it is a fact in cryptography that even the most secure technique is penetrated after a while. Hence a good software security engineer must always think of upgrading the security mechanism

CONCLUSION:

Currently phishing attacks are so common because it can attack globally and capture and store the user's confidential information. This information is used by the attackers which are indirectly involved in the phishing process. Phishing websites as well as human users can be easily identified using the proposed "Image CAPTCHA Authentication Based on Visual cryptography". The proposed methodology preserves confidential information of users using 3 layers of security. 1st layer verifies whether the website is a genuine/secure website or a phishing website. If the website is a phishing website (website that is a fake one just similar to secure website but not the secure website), then in that situation, the phishing website can't display the image CAPTCHA for that specific user (who wants to log in into the website) due to the fact that the image CAPTCHA is generated by the stacking of two shares, one with the user and the other with the actual database of the website. Second layer cross validates image CAPTCHA corresponding to the user. The image CAPTCHA is readable by human users alone and not by machine users. Only human users accessing the website can read the image CAPTCHA and ensure that the site as well as the user is the permitted one or not. So, using image CAPTCHA technique, no machine based user can crack the password or other confidential information of the users and as a third layer of security it prevents intruders' attacks on the user's account. This method provides additional security in terms of not letting the intruder log in into the account even when the user knows the username of a particular user. The proposed methodology is also useful to prevent the attacks of phishing websites on financial web portal, banking portal. Thus phishing is prevented effectively.

FUTURE SCOPE:

The number of conventional phishing attacks reported to the group rose from 14,987 in May to 15,050 in June. Meanwhile, the number of unique crimeware dedicated to password stealing doubled from 79 to 154 in the same period. These are some of the many facts that suffice to imply that the phishing attacks are prevalent all over the internet raising the risk of frauds done to all kinds of users ranging from laymen working with their bank accounts to the corporate people who deal with large amount of confidential information and financial transactions. This raises an alarm to both the sides of transaction, as the users would have their privacy and integrity as their outmost concern and the reputed organizations over the internet would always want to maintain their good will within their customers. Thus this project has a limitless scope in businesses of all domains active on the internet. With exponential increase in the deals over the net, 'Anti-phishing' mechanism is a security feature in high demand. It has its scope in the fields of e-commerce, e-banking and all such fields where monetary aspects and information transfer is involved. With further enhancement of this project from the commercial point of view, it will be market ready gaining customer confidence all over. This project can be enhanced further in future using face-detection techniques, 'image as password' technique and by numerous other such techniques which are planned to be implemented in near future. In future, this project has a potential to be market ready to provide protection for websites in all domains as mentioned earlier and that too, in all respects.

REFERENCE:

[1] A Novel Anti Phishing Framework Based on Visual Cryptography, 2012, Divya James, Mintu Philip.

[2] Anti-Phishing Group of the City University of Hong Kong.

[3] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12.

[4] Ollmann G., the Phishing Guide Understanding & Preventing Phishing Attacks, NGS Software Insight Security Research.

[5] Antiphishing Framework theglobaljournals.com/paripex

[6] C. M. Hu and W. G. Tzeng, .Cheating Prevention in Visual

[7] E. R. Verheul and H. C. A. Van Tilborg, .Constructions and Properties out of n Visual Secret Sharing Schemes, Designs, Codes, Cryptography, vol. 11, no. 2, 1997, pp. 179-196.

[8] A. Shamir, .How to Share a Secret, Communication ACM, vol. 22, 1979, pp. 612-613.