PREVENTION OF PHISHING ATTACKS IN VOTING SYSTEM USING VISUAL CRYPTOGRAPHY

Researchers :S.Supraja Arthi,P.Shakthy Abiraami.

Presentation title : Prevention of phishing attacks in voting system using visual cryptography.

Research focus :Password hygiene and Privileged Identity Management.

Institution :R.M.K. Engineering College.

Department :C.S.E -'C' 2nd year

Voting system Using Visual Cryptography (VC)aims at providing a facility to cast vote for critical and confidential internal corporate decisions. It has the flexibility to allow casting of vote from any remote place. The election is held in full confidentiality by applying appropriate security measures to allow the voter to vote for any participating candidate only if he logs into the system by entering the correct password which is generated by merging the two shares using VC scheme. Administrator sends share 1 to voter e-mail id before election and share 2 will be available in the voting system for his login during election. Voter will get the secret password to cast his vote by combining share 1 and share 2 using VC. Phishing is an attempt by an individual or a group to get personal confidential information from unsuspecting victims. Fake websites which appear very similar to the original ones are being hosted to achieve this. Internet voting focuses on security, privacy, and secrecy issues, as well as challenges for stakeholder involvement and observation of the process. A new approach is proposed for voting system to prevent phishing attacks.

METHODOLOGY:

For phishing detection and prevention, we are proposing a new methodology to detect the phishing website. The proposed methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography. It will allow only authenticated users to cast vote. Also it will prevent phishing attacks in the internet voting system

MODULES:

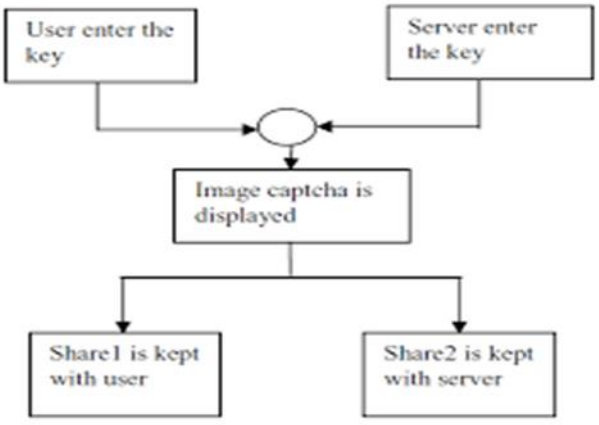
Registration: - In this module the admin will verify the user and register the user who will vote.

Send 1st share of password-As soon as the user registers the system will break the password and the first half of password will be sent to the users email-id and the 2nd share the user needs to enter while login.

Login: - This module enables the user and admin to login to the system by entering id and password.

New Candidate:- Admin will add the number of candidates nominated for Election whenever new election is announced.

Result: - Admin and user can view the election result by using the election id once the election results



Visual Cryptography:

Cryptography is an essential tool to protect the data that transmits between users by encrypting the data so that only intended users with appropriate keys can decrypt the data. It uses human visual system hence need not required a computer. They analyzed that the visual cryptography has two important

features: Cryptography is an essential tool to protect the data that transmits between users by encrypting the data so that only intended users with appropriate keys can decrypt the data. It uses human visual system hence need not required a computer. Therefore, visual cryptography is a very convenient way to protect secrets when computers or other decryption devices are not available. Cryptography is the most commonly used mechanism in protecting data. A survey conducted by Computer Security Institute in 2007 revealed that 71% of companies utilized encryption for their data in transit [3, 7]. Visual cryptography is first proposed by Nior and Shamir

- The first feature is its perfect secrecy .
- The second is its decryption method which requires neither complex decryption algorithms nor the aid of computers.
- The system can be used in various areas where election will be held

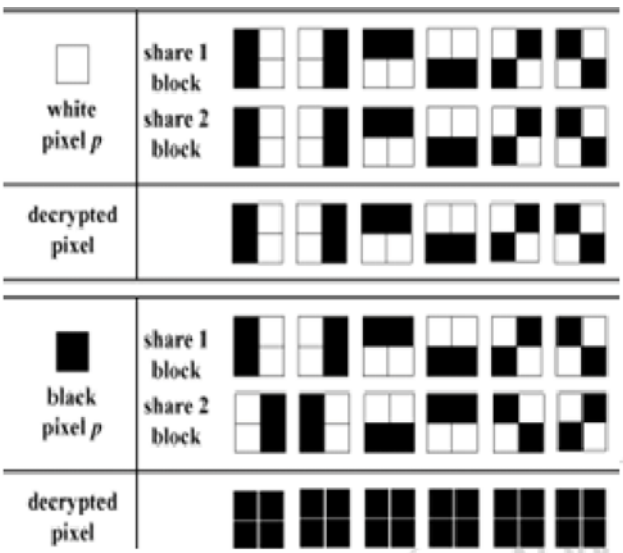


Figure 1: Construction of (2, 2) VC scheme: a secret pixel is

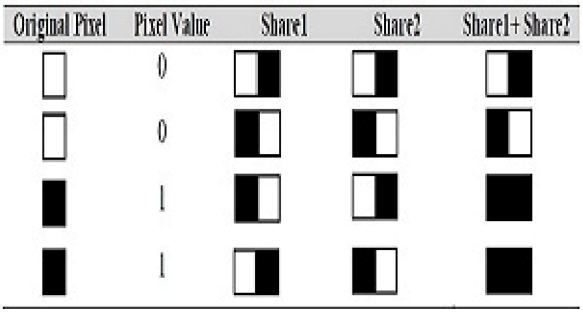
Various Visual Cryptography Schemes (VCS) The general construction of various visual cryptography schemes is as follows

1) **(2, 2) Threshold visual cryptography scheme:** In this scheme, a secret message and encrypts it in two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.

2) **(2, n) Threshold visual cryptography scheme**: This scheme encrypts the secret image into n shares such that when any two (or more) of the shares are overlaid the secret image is revealed. The user will be prompted for n, the number of participants.

3) **(n, n) Threshold visual cryptography scheme**: This scheme encrypts the secret image to n shares such that when all n of the shares are combined the secret image is revealed. The user will be prompted for n, the number of participants.

4) **(k, n) Threshold visual cryptography scheme:** This scheme says n shares will be produced to encrypt an image, and k shares must be stacked to decrypt the image. If the number of shares stacked is less than k, the original image is not revealed.



To analyze the security of the 2-out-of-2 VCS, the dealer randomly chooses one of the two pixel patterns (black or white) from the Table 1 for the shares S1 and S2. The pixel selection is random so that the shares S1 and S2 consist of equal number of black and white pixels. Therefore, by inspecting a single share, one cannot identify the secret pixel as black or white. This method provides perfect security. The two participants can recover the secret pixel by superimposing the two shared subpixels. If the superimposition results in two black subpixels, the original pixel was black; if the superimposition creates one black and one white sub-pixel, it indicates that the original pixel was white. In visual cryptography, the white pixel is representing by 0 and the black pixel by 1. Implementation of (2,2) is given below.

One Time Password (OTP):

One-time passwords are passwords that are used once and only valid for one login session or transaction. Banks, governments and other security based industries deploying OTP system where user may have many passwords and use each password only once. OTPs can avoid a number of shortcomings that are associated with traditional passwords which are valid for many transactions as users are reluctant to voluntarily change passwords frequently. Since OTPs are only valid for single use, an attacker has a smaller window of time to gain access to resources guarded by such a password because any previously stolen passwords will likely have become invalid.

There are mainly two types of password:

- Static password
- Dynamic Password

ADVANTAGES

- The system uses visual cryptography which enhances the security level of the system.
- The system will not allow the voter to vote two or more candidates.
- The system will allow the user to vote for one time for a particular election
- The system will authenticate the user through his fingerprint so the user is uniquely identified.

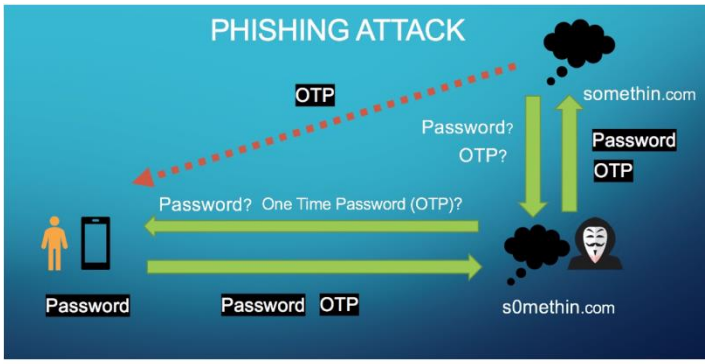


Figure 1

Conclusion:

Nowadays phishing has become one of the major issues and the number of phishing attacks is increasing more and more. Personal information is acquired in an electronic communication to cause financial losses. Lot of users becomes victim to these attacks. Hence s strong anti fishing mechanism is required. The proposed method preserves secret information of users. In this paper, anti fishing solution based on visual cryptography has been presented. Using proposed method, end user can easily identify the website is genuine or fake based on validation of image captcha. Additional security is provided by using OTP. 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 useful for financial web portal, banking portal and online shopping market to prevent the attacks of phishing websites.