International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 22 Issue 1 – MAY 2016.

SECURED AUTHENTICATION FOR INTERNET VOTING IN CORPORATE COMPANIES TO PREVENT PHISHING ATTACKS

Nisha S, Dr.A.Neela Madheswari

M.E. (CSE), CSE Department, Mahendra Engineering College, Namakkal, India

s.nish92@gmail.com
neela.madheswari@gmail.com

Abstract **- Corporations and organizations routinely use Internet voting to elect officers and Board members and for other proxy elections. Online voting refers to both the electronic means of casting a vote and the electronic means of tabulating votes. Using just a small sample of reported phishing content, a fairly good picture of which hosting providers may be more vulnerable to compromise or more forgiving of malicious behavior can be captured. This information can be useful when considering where to host the website or online service. Voting system with Visual Cryptography (VC) has been used for an efficient authentication of voting system to cast vote for confidential internal corporate decisions. Voters who bypass authentication or have already voted are denied access to the ballot. One-vote-per-voter is guaranteed by marking electors as voted and storing the vote in a single transaction. 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. A new approach is proposed to protect users across a network from phishing attacks.**

Keywords **- authentication, cryptography, image captcha, phishing, integer linear program, online voting**

I. INTRODUCTION

Fraudsters send fake emails or set up fake web sites that mimic. Phishing is a form of online identity theft in which fraudsters trick Internet users into submitting personal information to illegitimate web sites. Phishing scams are usually presented in the form of spam or pop-ups and are often difficult to detect. Once the fraudsters obtain your personal information, they can use it for all types of identity theft, putting your good credit and good name at risk. Phishers are becoming more and more sophisticated in designing their phony websites. Because phishing is one of the most devious forms of identity theft, it is important for you to become familiar with various types of phishing scams as well as to learn how to guard against them. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password [1].

Cryptography is the science of providing security for information. It has been used historically as a means of providing secure communication between individuals, government agencies, and military forces. Today, cryptography is a cornerstone of the modern security technologies used to protect information and resources on both open and closed networks [2].

Authentication is a process for verifying the identity of something or someone. When you authenticate an object, the goal is to verify that you have the genuine article. When you authenticate a person, the goal is to verify that you are not dealing with an imposter. Applications are required to implement their own mechanisms for determining the level of a user's authorization. Applications often do this by maintaining private lists that contain the names of users who are authorized access. Database applications, for example, often maintain private authorization tables to control the fields in a record that a particular user can view or change. There are different kinds of applications based on the Internet. One of them is online voting system. Several people advocate the benefits it can bring such as improved speed and accuracy in counting, accessibility, voting from home and as many are concerned with the risk it poses, such as unequal access, violation to secrecy and anonymity and alteration of the results of an election [3].

This paper focuses on the prevention of phishing attacks and secured authentication for Internet voting system using Visual Cryptography. The section II gives the detailed description of phishing techniques in general, section III explains the role of Visual Cryptography for anti-phishing, section IV explains the different kinds of voting systems, the section V proposed a new approach for Internet voting system with anti-phishing implementation and section VI concludes the proposal.

II. PHISHING TECHNIQUES

To prevent Internet phishing, users should have knowledge of various types of phishing techniques and they should also be aware of anti-phishing techniques to protect themselves from getting phished.

A. Email / Spam

Phishers may send the same email to millions of users, requesting them to fill in personal details. These details will be used by the phishers for their illegal activities. Phishing with email and spam is a very common phishing scam. Most of the messages have an urgent note which requires the user to enter credentials to update account information, change details, and verify accounts. Sometimes, they may be asked to fill out a form to access a new service through a link which is provided in the email.

B. Web Based Delivery

Web based delivery is one of the most sophisticated phishing techniques. Also known as "man-in-the-middle," the hacker is located in between the original website and the phishing system. The phisher traces details during a transaction between the legitimate website and the user. As the user continues to pass information, it is gathered by the phishers, without the user knowing about it.

C. Instant Messaging

Password Instant messaging is the method in which the user receives a message with a link directing them to a fake phishing website which has the same look and feel as the legitimate website. If the user doesn't look at the URL, it may be hard to tell the difference between the fake and legitimate websites. Then, the user is asked to provide personal information on the page.

D. Trojan Hosts

Trojan hosts are invisible hackers trying to log into your user account to collect credentials through the local machine. The acquired information is then transmitted to phishers.

E. Link Manipulation

Link manipulation is the technique in which the phisher sends a link to a website. When the user clicks on the deceptive link, it opens up the phisher's website instead of the website mentioned in the link. One of the anti-phishing techniques used to prevent link manipulation is to move the mouse over the link to view the actual address.

F. Key Loggers

Key loggers refer to the malware used to identify inputs from the keyboard. The information is sent to the hackers who will decipher passwords and other types of information. To prevent key loggers from accessing personal information, secure websites provide options to use mouse click to make entries through the virtual keyboard.

G. Session Hacking

In session hacking, the phisher exploits the web session control mechanism to steal information from the user. In a simple session hacking procedure known as session sniffing, the phisher can use a sniffer to intercept relevant information so that he or she can access the Web server illegally.

H. System Reconfiguration

Phishers may send a message whereby the user is asked to reconfigure the settings of the computer. The message may come from a web address which resembles a reliable source.

I. Content Injection

Content injection is the technique where the phisher changes a part of the content on the page of a reliable website. This is done to mislead the user to go to a page outside the legitimate website where the user is asked to enter personal information.

J. Phishing through Search Engines

Some phishing scams involve search engines where the user is directed to products sites which may offer low cost products or services. When the user tries to buy the product by entering the credit card details, it's collected by the phishing site.

K. Malware Phishing

Phishing scams involving malware require it to be run on the user's computer. The malware is usually attached to the email sent to the user by the phishers. Once you click on the link, the malware will start functioning. Sometimes, the malware may also be attached to downloadable files.

L. Website forgery and Covert Redirect

To avoid anti-phishing techniques that scan websites for phishing-related text, phishers have begun to use Flash-based websites. These look much like the real website, but hide the text in a multimedia object.

Covert Redirect is a subtle method to perform phishing attacks that makes links appear legitimate, but actually redirect a victim to an attacker's website. Covert Redirect is a notable security flaw. It is a threat to the Internet that is worth attention.

There is the possibility of occurrence of phishing in voting systems [4], and the social phishing scams have to be avoided or otherwise their effects can be easily wide spread in an election process. In the second quarter of 2015, the "Geography of phishing attacks", is given in figure 1 [5].

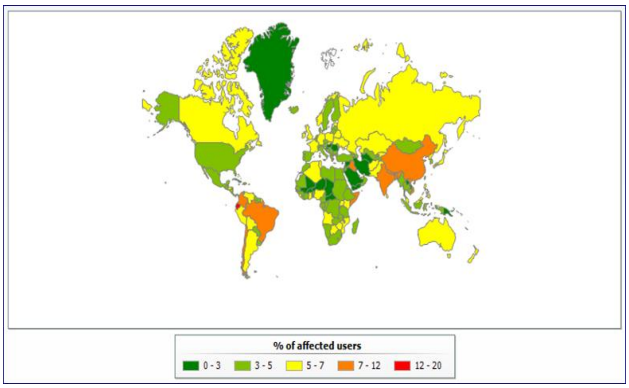

Fig. 1. Geography of Phishing attacks in second quarter of 2015

III. Visual Cryptography for Anti Phishing

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. There is a simple algorithm for binary (black and white) visual cryptography that creates 2 encrypted images from an original unencrypted image. The algorithm is as follows: First create an image of random pixels the same size and shape as the original image. Next, create a second image the same size and shape as the first, but where a pixel of the original image is the same as the corresponding pixel in the first encrypted image, set the same pixel of the second encrypted image to the opposite color. Where a pixel of the original image is different than the corresponding pixel in the first encrypted image, set the same pixel of the second encrypted image to the same color as the corresponding pixel of the first encrypted image. The two apparently random images can now be combined using an exclusive-or (XOR) to re-create the original image. When the random image contains truly random pixels it can be seen as a one-time pad system and will offer unbreakable encryption.

If Visual Cryptography is used for secure communications, the sender will distribute one or more random shares in advance to the receiver. If the sender has a message, he creates a share 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as both layers don't fall in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information.

IV. Evolution of Voting Systems

There are different types of voting systems starting from the early days and upto the current technological trends as shown in Fig. 2. These are explained in this section.

A. Paper ballot system

Paper ballot system is the commonly used traditional voting system. It is widely used before the introduction of electronic voting system. Paper ballot system includes casting the vote using the paper and the stamp. Each voter uses one ballot and it is not shared. The disadvantages in this system are: i) time consuming, ii) booth capture, iii) low tally speed.

B. Electronic voting system

An electronic voting system is a type of voting system which uses electronic ballot that would allow voters to broadcast their secret vote ballot to election officials over Internet. The disadvantages in this system are: i) persons poor in computer knowledge cannot vote proper, ii) vulnerable to security, iii) power consumption on the polling venue and iv) cost.

C. Online voting system

Online voting system is the latest electronic voting system introduced in which the voted ballot is transmitted over the public Internet through web browser. The voter can directly vote online from anywhere in the world. Security is the major drawback in using this system [7].

Some other related issues for online voting system based on security are:

- Most of the applications are giving high protection towards the Password Security and they are not concentrating on phishing attacks. By phishing, attackers are directly getting the passwords from the user and they can enter into the relevant web sites with correct password.
- There is no efficient technique to safe guard the users of phishing websites.

Other than the given voting systems, users can make use of other kinds of strategies for voting such as Newspaper voting, using social networks or from some other private networks also. But we cannot able to be sure that the voting is casted by proper authenticated users and hence these strategies cannot be used for voting purpose.

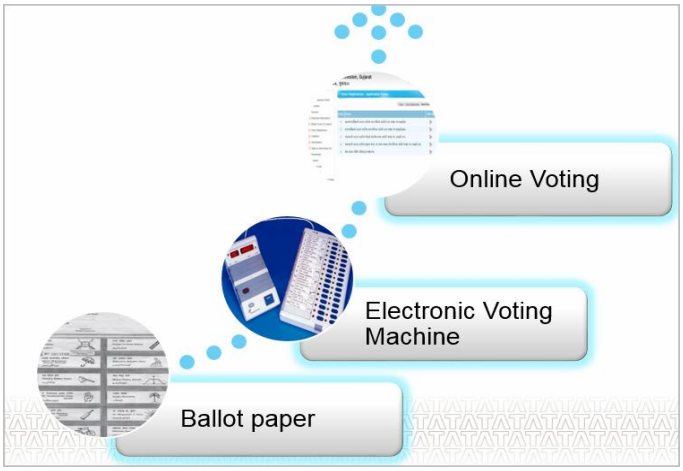

Fig. 2. Evolution of Voting Systems

V. Proposed Online Voting System

Consider an online polling system to elect the president or any other government authorities. As explained in section III, the mechanism for phishing detection and prevention can be done using the technique as described in figure 3.

Whenever the election officer or administrator in the case of any private concern who wants to perform voting upload the password image, it has to move from local system to web server. To divide the password image into two shares, this system proposed the Visual Cryptography technique.

Before dividing the image into two shares the image is first converted into Monochrome Image (Black and White Image).

Given a secret image S, a set P of n participants and a strong access structure, a Visual Cryptographic Scheme (VCS) for General Access Structures (GVCS) encodes S into n shares of transparencies. Modeling of minimizing the pixel expansion for a (k, n) - VCS into an integer linear program (ILP), to ensure that the constraints for GVCS can be satisfied. The pixel expansion of a GVCS can thus be minimized by solving the corresponding ILP. The proposed ILP is generalized for (*k, n)*-VCS. It can be applied to construct the basis matrices with the minimum pixel for a GVCS. The optimal pixel expansion of a GVCS can be acquired, especially for those applications that really need a GVCS with the smallest shares. After Image is divided into two shares one share has to be sent to the relevant voter through email, for which SMTP technique is used [8].

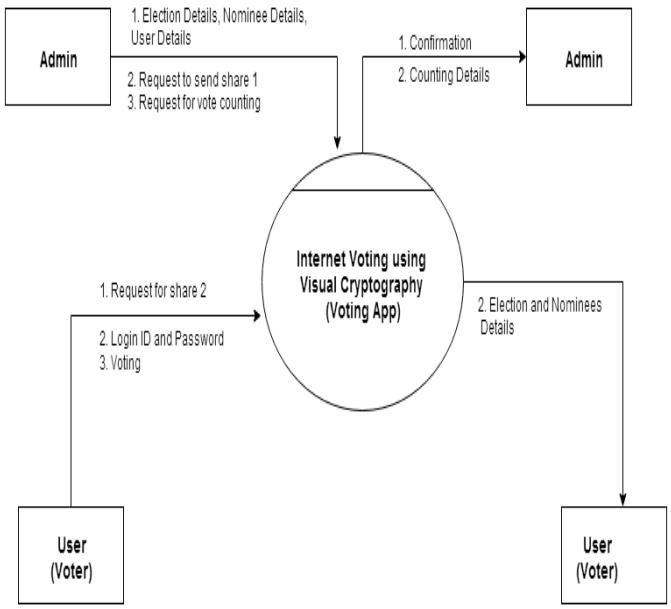

Fig. 3. Proposed Voting System using Visual Cryptography

The image of text captcha is split into two shares namely share1 and share 2. From Figure 3, we can easily identify three different forms of output. Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks. In case1 and case2, it is shown that correct images are formed and the captcha can be reconstructed properly whereas in case3, different shares are used and hence the captcha cannot be generated properly.

After entering the captcha, user is allowed to cast his vote. In case 3, the two shares are different and thus the output is not the proper image captcha. Hence user cannot able to enter the captcha and thus the user is logged out of the system.

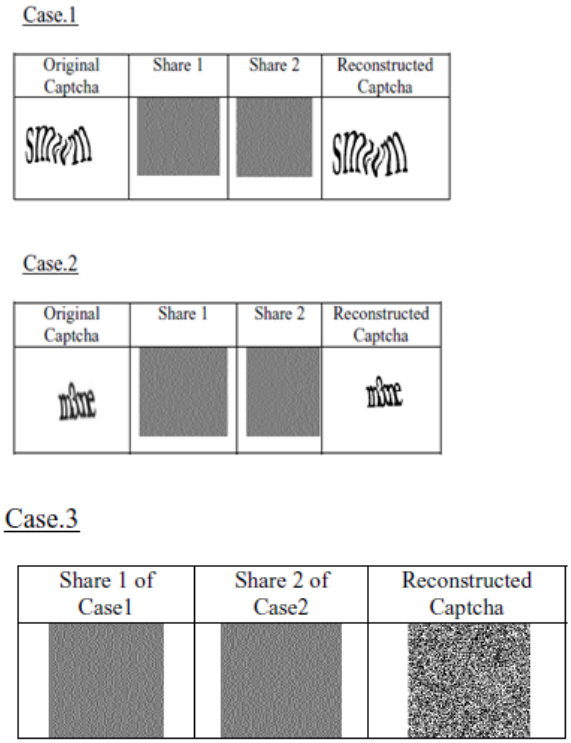

Fig. 3. Different cases of image captchas

For Online Polling system there should be many powerful validations to make the voting to be successful. Some of them are:

- Once voter did his polling, he should not be allowed to vote again. This can be accomplished by making his password to be expired.
- Whenever the voter did his polling, the corresponding voting count of that candidate has to be increased.
- Proper authentication should be provided so that the voters should not have unambiguous regarding the security of polling using online voting system. This can be achieved by the combined usage of visual cryptography and anti-phishing process.

Every voter should be provided with a share i.e. one of the image shares, of his password through any of the electronic

transfer system such as email. Proper mailing service should be provided to the voters with proper authentication. The voters have to make use of the same mailing system for receiving their shares using their mail ids already created by them in the corresponding mailing service.

There are two sessions involved in the proposed system. They are Admin session as shown in Fig. 5 and Voter session as shown in Fig. 6.

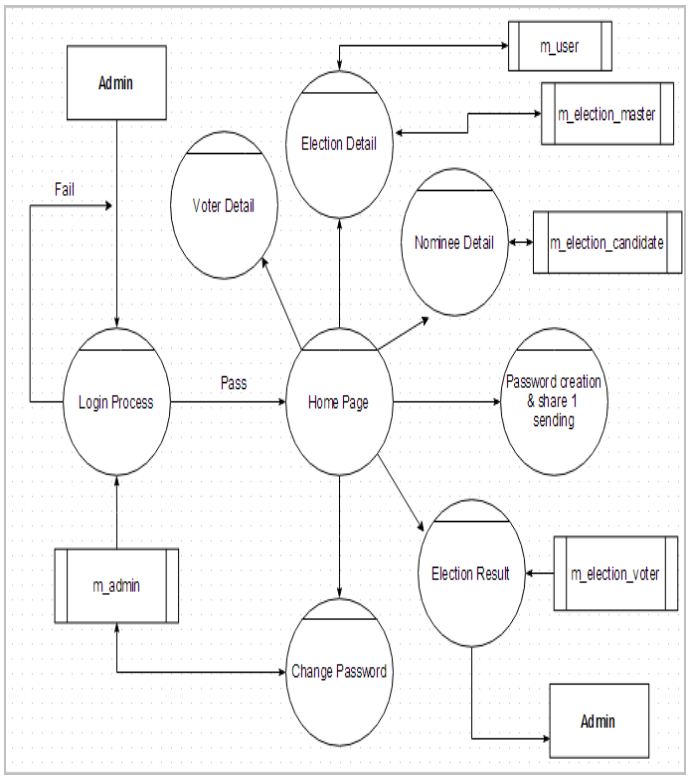

Fig. 5. Admin Session

Admin logins to the entire system and will be responsible for managing Voters Details, Election Details, Image Details (Text images), Nominees Details, Setting Voters Password, Election Counting Details and Change Password.

Voter session involves user login with phishing protection, providing User ID and getting Share from Server, Producing Captcha Image, and User Home Page were the user can Select Election, Display the Nominees, and cast the vote.

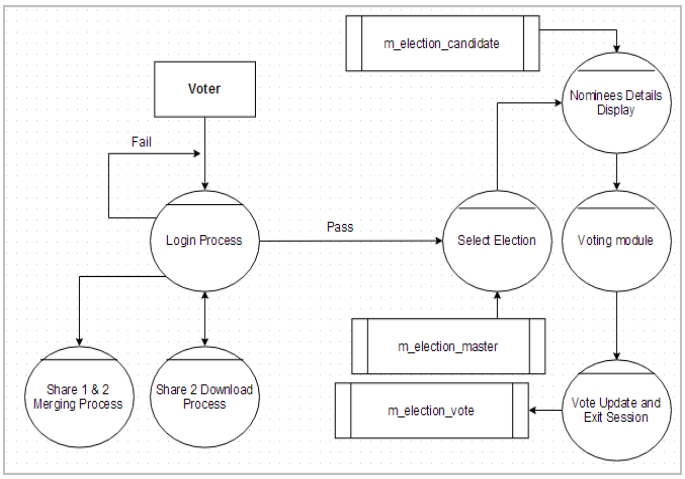

Fig. 6. User Session

VI. Conclusion

Voting plays an important role for any democratic country. If this proposal is implemented, then the voting percent can be improved further since few percent of our citizens are working in worldwide and they cannot able to come to native country at the time of voting. For those people as well as for the people who are physically disabled and very old also can make use of the online voting system. Since Visual Cryptography Technique is used, user can able to find out whether he is in phishing site or original site easily. Proposed online voting system is very effective and it will useful for voters and organization in many ways and it will reduce the cost and time.

References

[1] Network Security, https://en.wikipedia.org/wiki/Network_security, accessed on May 2015.

[2] Joey Paquet, http://users.encs.concordia.ca/~paquet/wiki/index.php?title=Capability_maturity_model, accessed on May 2015.

[3] Villafiorita A, Weldermariam K, Tiella R, "Development, Formal verification and evaluation of an e-voting system with VVPAT", IEEE Transactions on Information Forensics and Security, 2009, p.no. 651-661.

[4] Abdalla Al-Ameen and Samani Talab, "The Technical Feasiblity and Security of E-Voting", The International Arab Journal of Information Technology, Vol.10, No.4, July 2013, p.no.397-404.

[5] https://securelist.com/analysis/quarterly-spam-reports/69932/spam-and-phishing-in-the-first-quarter-of-2015/, Phishing attack, accessed on 12.09.2015.

[6] M. Mounika Reddy and B.Madhura Vani, "A Novel Anti phishing Framework based on Visual Cryptography", International Journal of Advanced Research in Computer and Communication Engineering, Vol.2, Issue 9, Sep 2013, P.No.3434-3436.

[7] Mayur Patil, Vijay Pimplodkar, Anuja R.Zade, Vinit Vibhute, Ratnakar Ghadge, "A Survey on Voting system techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue. 1, Jan 2013, p.no. 114-117.

[8] Shyong Jian Shyu, Ming Chiang Chen, "Minimizing Pixel expansion in Visual cryptographic scheme for General Access Structures", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 25, No. 9, Sep 2015.