International Journal of Advanced Engineering & Innovative Technology,
Volume 1, Issue 1, April-2014, 13-18 ISSN: 2348-7208

oPass mutual authentication system using visual cryptography

Dimble Prajakta G., Kadam Priyanka V., A.N. Kualage

B.E Computer Engineering, Navsahyadri Education Society's Group of Institutions, Pune.

For correspondence:dimbleprajakta@gmail.com, kadampriyanka2192@gmail.com , anant.kaulage@gmail.com

Abstract:

This paper proposes a method of providing security by using Visual Cryptography. Data access security is provided by this scheme. Visual Cryptography is applied to the password in the image captcha form & two shares are generated from this image-captcha. One share is placed on one server &another on the other server/user. This scheme provides security to the stored confidential data against malicious fake websites & online transactions. Since the shares are generated, which are not useful for the internal hackers.

Index Termse-commerce transaction Security, Captcha images, Malicious threat, share generation, Visual Cryptography.

Introduction:

Today, most applications are not much secure as their underlying system. Now day's people are used to do online transactions very commonly. But there are more security issues occur during online transaction, the major security threats are phishing attack, password reuse & stealing attack, brute force & dictionary attacks since the design and technology of malware has improved increasingly, detection of fake website or fake user, hacker is a difficult problem. As a result it is not possible to be sure whether a computer that is connected to the internet can be considered secure & trustworthy or not. The question arises, how to handle applications, that needs a high level of security, such as online banking. So to provide security the mechanism should be so effective, not easily tractable & with implementation easiness. In consequence we are interested in a solution that sure us to establish a trusted & secure communication, although the underlying system is untrusted.

In this paper we present an approach, which is based on Visual Cryptography. In [NaorS94] Shamir and Naor presented the concept of Visual Cryptography, which handles the plaintext to be encrypted as a graphic, which is processed pixel by pixel and thus gives interesting characteristics concerning security and fault tolerance. In [NaorP97] Naor and Pinkas demonstrated how to use Visual Cryptography for the authentication of one party without trusting the underlying system. Based on this, we developed a scheme for mutual visual authentication of a user and a server, which allows us to establish a trusted channel between the two parties, and can be used for secure communication. We describe the Visual Mutual Authentication - Scheme and demonstrate its application as a protocol on the example of online-banking. The protocol provides a practical and user-friendly approach to secure online banking, which is not only resilient to malware, but also resistant to phishing. Using Visual Cryptography, the user's key is a transparency that has to be applied on the computer monitor. With the transparency, the decrypted message can simply be read from the monitor by the user. We transfer this application to a VC-scheme and integrate a one-time pad structure. As a result, we achieve a user friendly scheme with a high level of secrecy. Customer data and program reside in Provider Premises so security concern arises. Following are the levels of providing security: 1) Server access security. 2) Internet access security. 3) Database access security. 4) Data privacy security. 5) Program access Security.

Text encryption/decryption methods like AES, RSA etc. are generally used for network security. We use Visual Cryptography in this paper to provide higher level of security. Visual Cryptography is a technique of encrypting a secret image into two or more shares [2]. The secret image can be decrypted by overlapping two or more shares. In conventional Visual Cryptographic scheme, the shares are random images having meaningless appearances. This may arouse the suspicion of hackers. Hence, in our method, nice-looking meaningful images are used as the covers to the shares.

The rest of the paper is organized as follows: section 2 introduces the proposed method for authentication using visual cryptography.Section3 gives the experimental results to show the effectiveness of this scheme and this paper is finalized in section 4.

Proposed system:

In this VC scheme, share generation, the random password i.e. OTP is given by user this OTP is then converted into image captcha. Two separate shares are generated of this image captcha. These shares are produced at server locations. During request session one share is given to the authenticated user by server. Although there is possibility of accessing a share by an unauthorized user at user side but because of OTP technique hacker, phisher fail to misused it. Single share cannot reveal the secret. Both the shares should be combined to decode the secret. The technique uses bitwise XOR operation to generate the visual shares. The generated shares are made by using the images captcha. This scheme involves two phases: Share generation and storing at different locations (encoding phase) and Secret image captcha recovery by combining the individual shares (decoding phase).

Encoding Phase:

The input is the random password i.e. OTP in the form of a black and white Secret image represented by matrix A of size m x n. The elements of A are 0's and 1's with 0 representing the black pixel and 1 the white pixel. Initial share sh1 is generated as a random image of 0's and 1's. The Second share, sh2 is generated by performing bitwise XOR operation of sh1 with the secret image A as follows.

sh1 = R1

(1) Where, R1 is a random binary matrix of size mxn.

sh2 =sh1 XOR A

(2) Where, Symbol represents bitwise XOR operation. The two shares generated are random looking shares and hence appear meaningless. Now from the property of XOR operation, it can be seen that, sh1 XOR sh2 =sh1 XOR sh1 XOR A= A

(3) Thus, combining sh1 and sh2 through XOR reveals A.

Algorithm 1: Share generation

This algorithm divides secret image into n number of shares. The shares created by this algorithm will be in unreadable format such that it is impossible to reveal secret image. Single share cannot reveal the secret image. If these individual shares are transmitted

Separately through communication network, security is achieved.

Input: A 2-Dimensional black and white secret image captcha A of size m x n.

Output: Two shares sh1 and sh2.

Procedure: SHARE GENERATION (A, B)

1. Get the first share sh1 as a binary random matrix as,
   sh1<- R1

2. Generate the second share sh2 by bitwise XORing the first share with the secret image as,
   sh2<- sh1 xor A

Symbol represents bitwise XOR operation.

3. Generate shares sh1 and sh2, once the two shares are ready, one share is stored in one server and the other share is stored in another server, not easily accessible from the first server.

Decoding Phase:

The decoding phase is performed by the legitimate user. He accesses the two shares from the two different servers and decodes the secret image by XORing the two meaningful shares. From and Eqs.

Sh1 XOR sh2= sh1 XOR D XOR sh2 XOR D =sh1 XOR sh2. (7)

From Eqs. (7) and (3),

Sh1 XORsh2= sh1 XOR sh2= A. (8)

The Decoding phase is given in Algorithm 2.

Algorithm 2: Decoding

This algorithm reveals the secret image by taking the number of shares as input. Some algorithm may take all shares as input and some other algorithm may take subset of shares as input. Decryption is done by merging shares which has taken as input

Input: Two shares sh1 and sh2.

Output: Decoded Secret image captcha.

Procedure: DECODE (sh1, sh2)

1. Decode the secret image A as,
   A<- sh1 XOR sh2

The proposed method provides data access security to the confidential data stored at the server site in cloud computing environment. Since the shares are meaningful, the inside malicious hackers do not pay any attention to it. Although a hacker gets to know one share, the other share is not easily accessible to him because other share is placed at another secured server, which is located far away. The confidential data, password cannot be decoded with only one share. So Good security is provided by this system.

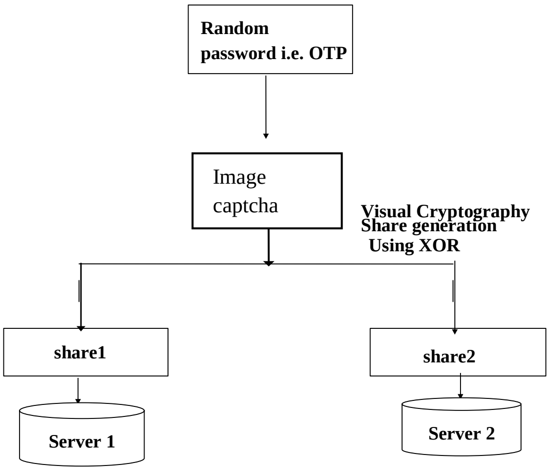


Fig.1:Encoding

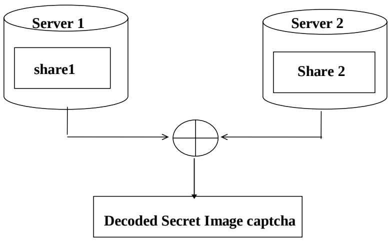


Fig.2.decoding

Experimental setup:

By applying this VC scheme, experimentally we demonstrate an example of to a credit card number or any confidential data like password. Credit card number or password is given as follows. This is going to be encrypted by generating captcha image. The inputs to encoding phase are the OTP. From this OTP The image captcha is generated

&by applying VC we generate two random looking shares.

One share is stored at one server and the other share is stored at the other far away server. In the decoding phase, the share1 & share2 are inputs which are XORed to obtain the secret image captcha given in

As a result we get Fig.3a and Fig.3d are the same. We observe from the experimental results that there is no quality loss in the decoded image. The non-expanded shares are provided by the proposed scheme. Advantage of this scheme is that implementation (using XOR) is simple and as compared to other encryption schemes like AES, RSA etc. it is robust.

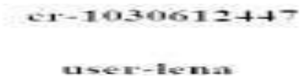
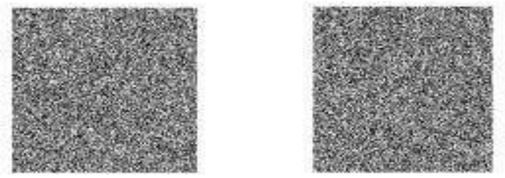


Fig.3a.:Secret Captcha.

.



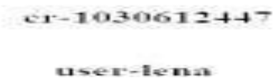


Fig.3d.: deconstructed secret Image captcha

Advantages:

Protection from malware:

Malware is a software it is used for destroy computer operation, it collect the secret information or gain access to private computer system. Malware includes the computer viruses, key logger, spyware etc. In oPass, malware cannot obtain all these sensitive information, so using oPass we can make our system malware free.

Phishing protection:

Online phishing is a way to rap computer users to give their personal or financial information through e-mail and website. In phishing any website or messages which look like original website or message. User cannot verify is this really phishing website and if they asked to provide personal information such as account number or password. This into is then usually used for identify theft. So our oPass given guarantee that user can verify the website where we do any transaction is real one or fake.

Preventing from reuse of password:

In general we create only one password for different login account we do not create different password. So hackers can easily hacked that password and because of only reuse of password he can login our all account where we using same password. Hence in oPass there is no need to use same password. OPass creates new password for each login.

In this way we can keep our email or other account free from hacker’s .Hacker cannot hack our password. For phishing detection & prevention, we are proposing a new methodology to detect the phishing website. Our methodology is based on the resistant to password stealing and password reuse attacks using visual cryptography. It prevents password and other confidential information from the phishing websites.

Resistance to phishing attacks:

Phishing is online identifying theft through phishing hacker, key logger hacked our information .but in oPass it can be detected phishing website .so we can do the transaction only with real website and we feel secure at the time of online transaction.

Weak password and remembrance:

Normally user create a password, which are easy to remember like family member name, pet name ,phone number etc. but hacker can guess this type of password. Therefore, in oPass user do not reuse same password for different accounts since generated.

SECURITY ANALYSIS

Protecting users from phishing attacks is very important. Phishing attacks means thieves the personal information like ATM PIN number, credit card information etc. SO we develop a new technology oPass: a user authentication protocol which provides us security.

Normally in traditional authentication system we have to enter user name and password then we can log into the system. So user always prefers to create short term password rather than long term password, but there are many possibilities of stealing these passwords easily. Normally user creates the password which is easy to remember. So this type of weak passwords can easily accessed by unauthorized person through dictionary attack.

Hence we develop oPass system which does the authentication by powerful, secure way. It gives guarantee to provide security.

The method of gaining access can be classified into parts based on attacker's targets which are user and server.

User side-

In this category, when user do the transaction with online website he don't know that website is phishing or real one. So he makes transaction by assuming that website is real. But may be that website can also be a fake. So our oPass system provides a mechanism to identified phishing website. Hence he can make a transaction on trusted website.

Server side-

In this category, when user does the transaction with online website that website is also doesn't know that user is fake or real. May be some unauthorized person steals the password of user and make a transaction. But by using oPass that website can get identify that which user is fake or authorized.

So in short, using our oPass system both user and server make a transaction more securely than using traditional authentication systems.

Related work:

In password based authentication, there are some problems like user create a weak passwords, they reuse the password for every accent and sometime they forgot their passwords. So text password based authentication is not very secure because of human behavior.

So to overcome this problem number of technologies are developed to reduce the unauthorized access of text passwords. The technologies developed are instead of text password use a graphical password .so by using graphical password technique users are at least remember there password.

Graphical password is easier than text based password for most people to remember .it provides better security than text password. But graphical password the user authentication system still suffers from some drawbacks and also it is not be used in practice. Next one technology is password management tool. In that these tools are created a random password which are strong password .there management tool works good, but the security is provided by them is not satisfactory. It consist lack of security knowledge. So after then a new technology is developed i.e. three factor authentication systems in that it include password, token and biometric. It provides a security but it requires a high cost, so normally users cannot use this technology. So, two factor authentication is cheaper than three factor authentication.

In many organizations they prefer a two factor authentication system .but it is still suffers from negative influences of human behavior that are reuse of password, weak password, forgot password etc. Hence for make our system, account secure there is need to more advanced technologies, which provide us best security.

In oPass, we use a visual cryptography to enhance the security and we think this requirement is reasonable and not costly. If we see performance it includes login, transaction and recovery phase which are executed within less time.

Future work:

Our oPass system provides a high level security by using a visual cryptography. But every system has some chances to become a powerful than any other system. So in our oPass system future developments include a more user friendly GUI and also use more effective encryption algorithm. So password can be generated based on different ways to authenticate system.

Conclusion:

Now a day's phishing attacks are become a serious problem. In phishing attack they capture our personal information like, credit card information, ATM pin number, password etc. So user are suffers from these phishing attacks.

Hence there is need to identified phishing website and this can be done by using our developed system oPass by using visual cryptography technique. In that captcha image is used for generating two shares. One share is placed on one server and another on the other server. In this way mutual protection is provided by the system from phishing attacks & it can resist to unauthorized person from stealing confidential data , password etc.

So our proposed system methodology is useful to prevent the attacks of phishing website on financial web portal, banking portal, online shopping market etc.

References:

[1]Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin "oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks". IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.

[2] M. Naor and A. Shamir, "Visual cryptography," Proceedings of Advances in Cryptology: Eurocrypt94, Lecture Notes in Computer Science, Vol. 950, pp. 1 - 12, 1995.

[3] Xiaoqing GU, Hongyuan WANG∗, Tongguang NI School of Information Science and Engineering, Changzhou University, Changzhou 213064, China." An Efficient Approach to Detecting Phishing Web ⋆". Journal of Computational Information Systems 9: 14 (2013) 5553–5560.

[4] Daphna Weinshall School of Computer Science and Engineering The Hebrew University of Jerusalem, Jerusalem, Israel 91904," Cognitive Authentication Schemes for Unassisted Humans, Safe Against Spyware". Hebrew University Leibniz Center for Research in Computer Science TR 2006-5, 2006.

[5] Haijun Zhang, Gang Liu, Tommy W. S. Chow, Senior Member, IEEE, and Wenyin Liu, Senior Member, IEEE." Textual and Visual Content-Based Anti-Phishing: A Bayesian Approach". IEEE TRANSACTIONS ON NEURAL NETWORKS, VOL. 22, NO. 10, OCTOBER 2011.

[6] P. Vaisagan, M., Nasreen Fathima, P.Elenthendral," Web Based Security Analysis of oPass Authentication Scheme Using Mobile Application". IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013 ISSN: 2320 – 8791.

[7] Divya James, and Mintu Philip, MTech in Information System Security, Indira Gandhi National Open University, India," A NOVEL ANTI PHISHING FRAMEWORK BASED ON VISUAL CRYPTOGRAPHY". International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012.

[8]Ms. R.R.Karthiga, Mr.K.Aravindhan," Enhancing Performance of User Authentication Protocol with Resist to Password Reuse Attacks". International Journal of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 8.