International Journal on Applications in Information and Communication Engineering
Volume 2: Issue 2: Feburary 2016, pp 11-15. www.aetsjournal.com ISSN (Online) : 2394-6237

A Robust User Authentication Scheme For Webapplications Using Visual Cryptography Techniques

R.Anita Ruth Sweetlin

Abstract— Visual cryptography is a cryptographic technique that allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. Security images are often used as part of the login process in many web applications. Eg. Internet banking websites. These images can help foil several cyber-attacks. Phishing is an attack attempted by an individual or a group to thieve personal confidential information such as passwords, credit card information etc. from unsuspecting victims for identity theft, financial gain and other fraudulent activities. The first defence mechanism against such attacks is strengthening the authentication mechanism in a web application. A simple username and password based authentication is not sufficient for web sites providing critical financial transactions. Security images are one type of visual securityindicator. Others include special toolbars and SSL warnings.

In this paper we have proposed a new approach of user authentication that also handles the problem of phishing. Phishing websites comprise a variety of cues within its content-parts as well as the browser-based security indicators provided along with the website.The use of images is explored to preserve the privacy of image captcha by decomposing the original image captcha into two shares that are stored in separate database servers, such that,the original image captcha can be revealed only when both are simultaneously available; the individual sheet images do not reveal the identity of the original image captcha. Once the original image captcha is revealed to the user it can be used as the password. Several solutions have been proposed to tackle phishing.

I. INTRODUCTION

A. VISUAL CRYPTOGRAPHY

Visual cryptography is acryptographictechnique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer.a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image.

Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear.

B. IMAGE CAPTCHA

A CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a type of challenge response test used in computing to determine whether or not the user is human. This form of CAPTCHA requires that the user type the letters of a distorted image, sometimes with the addition of an obscured sequence of letters or digits that appears on the screen. Because the test is administered by a computer, in contrast to the standard turing test that is administered by a human, a CAPTCHA is sometimes described as a reverse Turing test. This term is ambiguous because it could also mean a Turing test in which the participants are both attempting to prove they are the computer.

C. USER AUTHENTICATION

The act of confirming the truth of an attribute of a single piece of data claimed true by an entity. In contrast with identification which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. It might involve confirming the identity of a person by validating their identity documents, verifying the authenticity of a website with a digital certificate, determining the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labeling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification.

D. WEB APPLICATION

Aweb applicationorweb appis aclientserversoftware applicationin which the client (or user interface) runs in aweb browser Web applications are popular due to the ubiquity of web browsers, and the convenience of using a web browser as aclientto update and maintain web applications without distributing and installing software on potentially thousands of client computers is a key reason for their popularity, as is the inherent support for cross-platform compatibility. Common web applications includewebmail, online retail sales,online

R.Anita Ruth Sweetlin, *M.E CSE 2nd Year,Fatima Michael College of Engineering and Technology,Madurai.*

auctions,wikis,instant messaging servicesand many other functions.

II. LITERATURE SURVEY

A literature review is a text of a scholarly paper, which includes the current knowledge including substantive findings, as well as theoretical and methodological contributions to a particular topic. Literature reviews use secondary sources, and do not report new or original experimental work.

A. Robert Biddle, Sonia Chiasson, P.C. van Oorschot., "Graphical Passwords: Learning from the First Twelve Years", January 4, 2011.

Starting around 1999, a great many graphical password schemes have been proposed as alternatives to text-based password authentication. We provide a comprehensive overview of published research in the area, covering usability and security aspects, as well as system evaluation. The paper first catalogues existing approaches, highlighting novel features of selected schemes and identifying key usability or security advantages. We then review usability requirements for knowledge-based authentication as they apply to graphical passwords, identify security threats that such systems must address and review known attacks, discuss methodological issues related to empirical evaluation, and identify areas for further research and improved methodology.

B. Alain Mayer, Fabian Monrose, Michael K. Reiter, "The Design and Analysis of Graphical Passwords", August 23–26, 1999.

In this paper we propose and evaluate new graphical password schemes that exploit features of graphical input displays to achieve better security than text-based passwords. Graphical input devices enable the user to decouple the position of inputs from the temporal order in which those inputs occur, and we show that this decoupling can be used to generate password schemes with substantially larger (memorable) password spaces. In order to evaluate the security of one of our schemes, we devise a novel way to capture a subset of the memorable" passwords that, we believe, is itself a contribution. In this work we are primarily motivated by devices such as personal digital assistants (PDAs) that graphical input capabilities via a stylus, and we describe our prototype implementation of one of our password schemes on such a PDA, namely the Palm PilotTM.

C. Susan Wiedenbecka, Jim Watersa, Jean-Camille Birget, Alex Brodskiyc, Nasir Memonc, "PassPoints:Design and longitudinal evaluation of a graphical password system.", January 14, 2005.

Computer security depends largely on passwords to authenticate human users. However, users have difficulty remembering passwords over time if they choose a secure password, i.e. a password that is long and random. Therefore, they tend to choose short and insecure passwords. Graphical passwords, which consist of clicking on images rather than typing alphanumeric strings, may help to overcome the problem of creating secure and memorable passwords. In this paper we describe Pass Points, a new and more secure graphical password system. We report an empirical study comparing the use of Pass Points to alphanumeric passwords. Participants created and practiced either an alphanumeric or graphical password. The participants subsequently carried out three longitudinal trials to input their password over the course of 6 weeks. The results show that the graphical password users created a valid password with fewer difficulties than the alphanumeric users. However, the graphical users took longer and made more invalid password inputs than the alphanumeric users while practicing their passwords. In the longitudinal trials the two groups performed similarly on memory of their password, but the graphical group took more time to input a password.

D. P.C. van Oorschot, Julie Thorpe, "Predictive Models and User Drawn Graphical Passwords.", June 2, 2007.

In commonplace text-based password schemes, users typically choose passwords that are easy to recall, exhibit patterns, and are thus vulnerable to brute-force dictionary attacks. This leads us to ask whether other types of passwords (e.g., graphical) are also vulnerable to dictionary attack due to users tending to choose memorable passwords. We suggest a method to predict and model a number of such classes for systems where passwords are created solely from a user's memory. We hypothesize that these classes define weak password subspaces suitable for an attack dictionary. For user-drawn graphical passwords, we apply this method with cognitive studies on visual recall. These cognitive studies motivate us to define a set of password complexity factors (e.g., reflective symmetry and stroke-count), which define a set of classes. To better understand the size of these classes, and thus how weak the password subspaces they define might be, we use the "Draw-ASecret" (DAS) graphical password scheme of Jermyn et al. (1999) as an example. We analyze the size of these classes for DAS under convenient parameter choices, and show that they can be combined to define apparently popular subspaces that have bitsizes ranging from 31 to 41 – a surprisingly small proportion of the full password space (58 bits). Our results quantitatively support suggestions that user-drawn graphical password systems employ measures such as graphical password rules or guidelines, and proactive password checking.

E. Ahmet Emir Dirik, Nasir Memon, Jean-Camille Birget, "Modeling user choice in the PassPoints graphical password scheme."July 18-20, 2007.

We develop a model to identify the most likely regions for users to click in order to create graphical passwords in the PassPoints system. A PassPoints password is a sequence of points, chosen by a user in an image that is displayed on the screen. Our model predicts probabilities of likely click points; this enables us to predict the entropy of a click point in a graphical password for a given image. The model allows us to evaluate automatically whether a given image is well suited for the PassPoints system, and to analyze possible dictionary

attacks against the system. We compare the predictions provided by our model to results of experiments involving human users. At this stage, our model and the experiments are small and limited; but they show that user choice can be modeled and that expansions of the model and the experiments are a promising direction of research.

F. Julie Thorpe and P.C. van Oorschot, "Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords.", August 6-10, 2007.

Although motivated by both usability and security concerns, the existing literature on click-based graphical password schemes using a single background image(e.g., PassPoints) has focused largely on usability. We examine the security of such schemes, including the impact of different background images, and strategies for guessing user passwords. We report on both short- and long-term user studies: one lab-controlled, involving 43 users and 17 diverse images, and the other a field test of 223 user accounts. We provide empirical evidence that popular points (hot-spots) do exist for many images, and explore two different types of attack to exploit this hot spotting:(1) a "human-seeded" attack based on harvesting click-points from a small set of users, and (2) an entirely automated attack based on image processing techniques. Our most effective attacks are generated by harvesting password data from a small set of users to attack other targets. These attacks can guess 36% of user passwords within 231 guesses (or 12% within 216 guesses) in one instance, and 20% within 233 guesses (or 10% within 218 guesses) in a second instance. We perform an image-processing attack by implementing and adapting a bottom-up model of visual attention, resulting in a purely automated tool that can guess up to 30% of user passwords in 235 guesses for some instances, but under 3% on others. Our results suggest that these graphical password schemes appear to be at least as susceptible to offline attack as the traditional text passwords they were proposed to replace.

III. SYSTEM ANALYSIS

A. PROBLEM DEFINITION

Online transactions are now very common and the applications used for those are subjected to several cyber-attacks. Among these attacks, phishing is identified as a major security threat and new innovative ideas are arising to tackle it. Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Phishing scams are becoming a big problem for online banking and e-commerce users.

So, the need of the hour is to provide a high level of security and strengthen the authentication mechanisms. Prevention is always better than cure. The same should not be easily traceable with implementation easiness. Today, most applications are only as secure as their underlying system. Though the design and technology of underlying softwares and hardwares have improved steadily, detecting a threat is a difficult problem. As a result, it is nearly impossible to be sure whether a computer that is Here we propose a new method to strengthen the authentication based on the relation of Random Grid and Deterministic Visual Cryptography. As the name describes, in this approach website cross verifies its own identity and proves that it is a genuine website and also authenticates the users thereby making both the sides of the system secure as well as an authenticated one. The concept of image processing and an improved visual cryptography is used. Image processing is a technique of processing an input image and to get the output as either improved form of the same image and/or characteristics of the input image. Visual Cryptography (VC) is a method of encrypting a secret image to shares, such that stacking a sufficient number of shares reveals the secret image. The main objective is to verify the identity of the application as well as users by the proposed user authentication scheme.

B. EXISTING SYSTEM

1) Blacklist-based technique

In computing, a blacklist or block list is a basicaccess control mechanism that allows through all elements (email addresses, users, URLs, etc.), except those explicitly mentioned. Those items on the list are denied access. The opposite is a whitelist, which means only items on the list are let through whatever gate is being used. A greylist contains items that are temporarily blocked (or temporarily allowed) until an additional step is performed. For example, a company might prevent a list of software from running on its network or a school might prevent a list of web sites from being accesses on its computers.

Limitations

- Low false alarm probability.
- Cannot detect the websites that are not in the blacklist database.
- Accuracy is not too high.

2) Heuristic-based anti-phishing technique

Heuristic-based anti-phishing technique is to estimate whether a page has some phishing heuristics characteristics. For example, some heuristics characteristics used by the Spoof Guard toolbar include checking the host name, checking the URL for common spoofing techniques, and checking against previously seen images. If you only use the Heuristic-based technique, the accuracy is not enough. Besides, phishers can use some strategies to avoid such detection rules. The user may be deceived by the phishing website because the phishing website imitates a legitimate website. Its pages are often similar with the legitimate sites.

Limitations:

- High probability of false and failed alarm.
- It is easy for the attacker to use technical means to avoid the heuristic characteristics detection.
- Detecting phishing websites on the client terminal is not

suitable.

- Low accuracy rate.

C. PROPOSED SYSTEM

Our proposed methodology is an image based authentication using Visual Cryptography is implemented. The use of visual cryptography is explored to preserve the privacy of an image captcha by decomposing the original image captcha into two shares (known as sheets) that are stored in separate database servers(one with user and one with server) such that the original image captcha can be revealed only when both are simultaneously available; the individual sheet images do not reveal the identity of the original image captcha. Once the original image captcha is revealed to the user it can be used as the password. Using this website cross verifies its identity and proves that it is a genuine website before the end users.

1) PSEUDO-RANDOM NUMBER GENERATOR:

PRNG, is a random number generator that produces a sequence of values based on a seed and a current state.

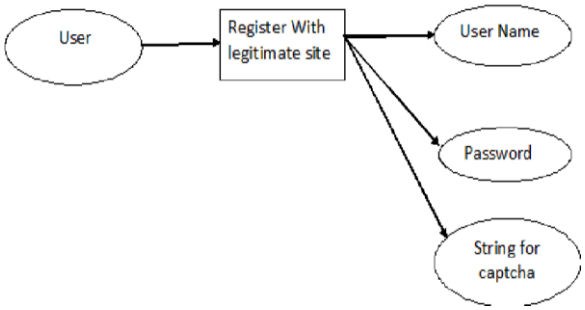
- A seed (starting value) s is chosen.
- A hash function f (s) is applied repeatedly (for example, 1000 times) to the seed, giving a value of: f (f (f (.... f (s) ....))). This value, which we will call f 1000(s) is stored on the target system.
- The user's first login uses a password p derived by applying f 999 times to the seed, that is, f 999(s). The target system can authenticate that this is the correct password, because f (p) is f 1000 (s), which is the value stored. The value stored is then replaced by p and the user is allowed to login.

2) RANDOM PATTERN ALGORITHM:

Random pattern algorithms to encrypt a binary secret image. The input of the algorithm is a w × h image, denoted by A, and the outputs are two images R1 and R2.

The encryption procedure encrypts a secret image into the shares(printed on transparencies)which are noiselike secure images Which can be transmitted or distributed over an untrusted communication channel.

IV. DATA FLOW DIAGRAMS



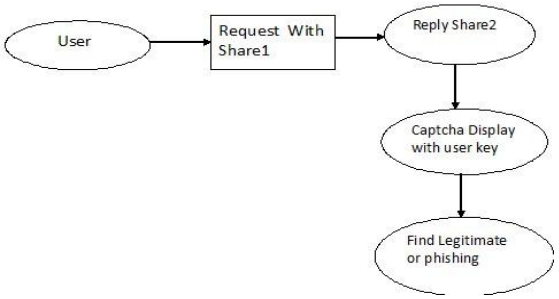


FIG. 4.1 User Registration

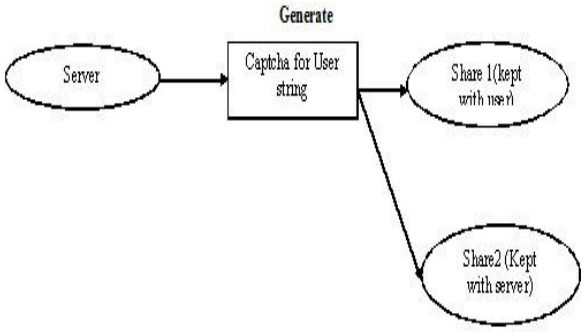
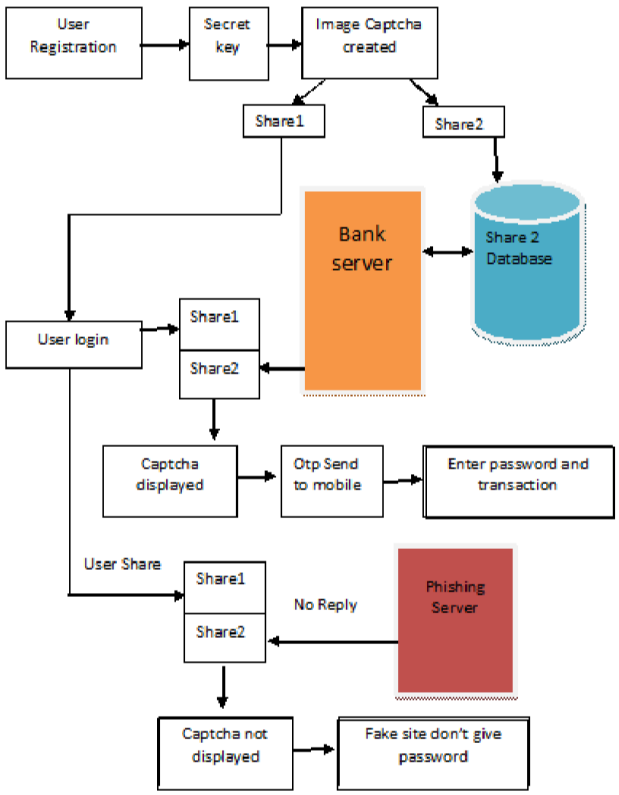


FIG. 4.2 IMAGE DATAFLOW DIAGRAM CAPTCHA

V. SYSTEM ARCHITECTURE



VI. MODULES

A. Registration with Secret Code:

- The user details and a key string (password) are 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.

B. Image Captcha Generation:

- A key string is converted into image using java classes BufferedImage and Graphics2D.
- The image dimension is 260*60. Text color is red and the background color is white.
- Text font is set by Font class in java.
- After image generation it will be write into the userkey folder in the server using ImageIO class.

C. Shares Creation (VCS):

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

D. Login Phase:

When the user logs in by entering his username (user id) the user is asked to enter his share of captcha. This share is sent to the server where the user's share is stored in the database of the website for each user. These are 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 becomes the password and using the same the user can log in into the website. Also using the image captcha generated by stacking two shares one can verify whether the website is genuine/secure website or a phishing website.

VII. CONCLUSION & FUTURE ENHANCEMENT

A. CONCLUSION

Cyber frauds are increasing day by day. Intelligent attackers are creating fake websites that are same as the original/genuine websites and thereby capture,store user's confidential information. By using the proposed scheme it is possible to overcome the above scenario. The scheme helps to recognize if the system is genuine or not. The use of shares as a security key increases the security level. This can be used in sectors like banking, finance and online shopping.

B. FUTURE ENHANCEMENT

In future we can increase the security by adding many algorithms to encrypt the image. Encryption Phase contains many algorithms like Blowfish, Splitting and Rotating algorithm and (2,2) Visual Cryptography Scheme.

First the "Blowfish Algorithm" is applied to the original image captcha then the image captcha is divided into many blocks and rearranged. After the image captcha blocks are rearranged, the "Splitting and Rotating Algorithm" is applied to the image captcha, and then the rearranged blocks are rotated.

Then the rearranged and rotated blocks are combined. Then (2, 2) VCS scheme is applied to the combined blocks.

This scheme is used to divide the encrypted image captcha into two shares based on white and black pixels. When the two sub pixels are identical blocks it considers as a white pixel. Likewise when the two sub pixels are different the original pixel is considered as black pixel. This VCS scheme adds more complication to the image captcha.

REFERENCES

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys, vol. 44, no. 4, 2012.
[2] The Science Behind Passfaces [Online]. Available: http://www.realuser.com/published/Science BehindPassfaces.pdf
[3] Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proc. 8th USENIX Security Symp., 1999, pp. 1–15.
[4] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292, 2008.
[5] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," Int. J. HCI, vol. 63, pp. 102–127, Jul. 2005.
[6] P. C. van Oorschot and J. Thorpe, "On predictive models and userdrawn graphical passwords," ACM Trans. Inf. Syst. Security, vol. 10, no. 4, pp. 1–33, 2008.
[7] K. Golofit, "Click passwords under investigation," in Proc. ESORICS, 2007, pp. 343–358.
[8] E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in Proc. Symp. Usable Privacy Security, 2007, pp. 20–28.
[9] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot spots in graphical passwords," in Proc. USENIX Security, 2007, pp. 103–118.
[10] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on passpoints-style graphical passwords," IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 393–405, Sep. 2010.