Efficacy of Object-Based Passwords for Student Authentication Framework for Online Examination

J.Suneetha[1], K.Venkata Ramana[2]
[1] *Student, Dept. of MCA, KMM Institute of Post Graduate Studies*
[2] *Assistant Professor, Dept. of MCA, KMM Institute of Post Graduate Studies, Tirupati,A.P*

Abstract- **In the recent years, net has become more and more widespread and utilized by many folks from everywhere the world. Online learning is wide acceptable. Online examination could be a basic a part of online learning. Student work and assessment is remotely submitted with none face to face interaction. Student could submit already submitted work thus originality of fabric is greatly defeated. So Student authentication in online examination is seen as a 1 of the foremost problem and challenges. This paper proposed the novel student authentication framework for on-line examination. During this paper, we have a tendency to extend the ObPwd theme with a brand new object primarily based password theme that performs majority of the computation at the server facet. This paper basically discusses 2 frameworks for object password schemes, an object hash-based theme (where the shopper machine computes the hash of the object to be used as text password) and an object-based theme (where the thing is directly transmitted to the server as password). We conjointly evaluate the performance of both the thing password schemes against standard text-based password schemes using prototypes of every of the frameworks. Implications with relevancy simple use, sharing and security also are mentioned.**

Index Terms- **Object-based Passwords, Passwords, object-hash based scheme.**

I. INTRODUCTION

NOW a day's world may be a net world. Many folks from all over the planet uses the net to transmit their confidential information over the communication network.Nowdys on-line learning has become more and more in style. On-line examination play terribly very important role in on-line education. On-line education material is well accessible and wide updatable. Hence various instructional institute, banking sector adopt this in giant scale. Within the on-line examination situation, there's no face to face interaction between students and system directors. so security has become necessary issue during this situation. Throughout on-line examination, students submit their work remotely. Therefore it becomes troublesome to verify the identity of person taking on-line examination. Students might submit plagiarize work as a part of their assessment. Student imitates or uses the first work of alternative author. Therefore plagiarism will be one of the main challenges to on-line learning. On-line learning offer a lot of opportunities for cheating and tutorial dishonesty in such examination. Cheating in on-line examination looks to

Be terribly serious issue. Therefore there's necessity of a lot of reliable and secure student authentication system. Users pay insufficient attention to wisely choose a password. This tendency has been exploited using simple attacks like password guessing to more specialized methods such as dictionary attacks. The loopholes of text-based passwords are well documented. It is also difficult for users to generate and memorize strong or high-entropy passwords. Further, these strong passwords are generally usable only if they are frequently used. Passwords for rarely-used services are hard to reproduce at a later point in time.

II. RELATED WORK

It allows users to generate passwords from digital content that may range from a personal collection of photographs to static content from the web. The Internet Archive (www.archive.org) and Google Books (books.google.com) were recognized as good object selection pools. A prototype browser based plugin was developed that computed object hashes on the client machine. The resulting hash string could be copied to the clipboard and used as a text-based password by the user. It allows the hash to be

recorded (because of its textual nature) on any medium, and also allowed the hash to be recomputed, provided the same object could be reproduced by the user.

In this paper, we extend *ObPwd* scheme with a new object based password scheme that offloads majority of computation at the server side. This approach is beneficial for the low end client machines with insufficient processing power. Numerous efforts have been made over the years by the scientific community to strengthen passwords and to enhance their usability. A few noteworthy efforts include [5], [6], [9], [15], [16], [19], [20], [21]. In this section we have primarily focused on the most relevant object based password scheme.

The idea of using digital objects as password was first realized in *ObPwd* by Mannan et.al. [29], [30].

III. PROPOSED FRAMEWORK DESIGN AND PROTOTYPE

We have developed prototypes of three different password schemes; 1) text-based, 2) object hash-based and 3) object based. The framework design and prototypes are discussed in the following subsections.

TEXT-BASED PASSWORD SCHEME

Text-based passwords have been used since ancient times to allow (or disallow) a person or group to enter an area. They have since been adopted by information system designers to serve the same purpose of authentication and gaining access to a resource.

Fig. 1 shows how a standard text-based password scheme is realized to authenticate any user over the web. A user supplies their credentials (a user-ID and password) through a web form to authenticate them to an information system and to gain access to its online services. The userID and password are delivered to the authenticating web server, which then decides whether the supplied credentials are correct or incorrect.

While spoofing may be mitigated using SSL, text-based passwords still leave the door open for many other attacks. Most of these attacks arise because of the user's choice of passwords. Text-based passwords actually have to be remembered, imposing a memory load on the user that they would otherwise wish to avoid. Enterprises place various restrictions on the user's choice of password (length, numeric or special characters) so that they may choose stronger, more secure passwords. This technique is not very effective however, as users still look for the easiest password they can construct given the restrictions. Meanwhile attackers can compute special tables with most common user passwords and use them to break into user accounts.

For the prototype of text-based scheme, the server maintains a list of user-IDs and their respective password hashes in a database. Passwords are not stored as plain-text to account for any possibility of the database being compromised, in which case the attacker would have access to every user account on the system. An attacker may still however employ rainbow tables to crack these password hashes, and to mitigate such an attack, a key derivation function using salts is employed. A salt is a randomly generated string that is generated with each new user account that is created.

Upon an authentication request, the server fetches the corresponding password hash and salt stored against the userID. It then concatenates the salt with the password, computes the hash and validates it against the hash fetched from the database. The cryptographic hash function utilized here is SHA-256, from the SHA-2 family.

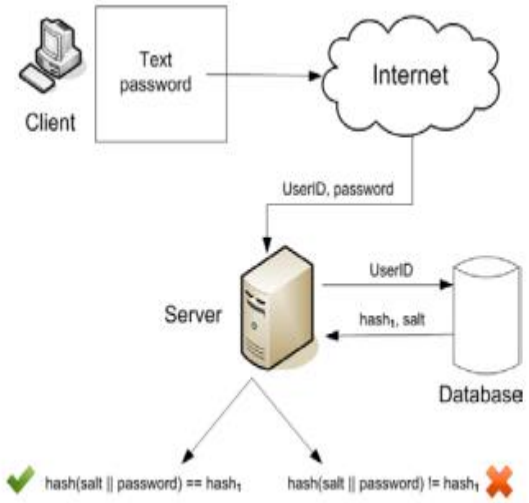

Fig. 1 Text-Based Password Scheme.

OBJECT HASH-BASED PASSWORD SCHEME

The object hash-based password scheme employs media objects as user's passwords and performs majority of the computation on the client using client-side scripts. As it can be seen from Fig. 2, the

server side functionality is consistent with that of the text-based password scheme. The server receives the user-ID and a text-based version of the user password (hash of the media object), fetches the password hash and salt from the database and evaluates whether the received credentials are valid.

This scheme allows the user to maintain a text-based version of their chosen media object on a non-digital medium, in case their media object is unavailable at any point in time. This would be highly useful if and when the media object were to become corrupted, and also when the user would be trying to gain access to a service from a system not of their own, and the media object would either be unavailable or could possibly be compromised if loaded on a 3rd party computer.

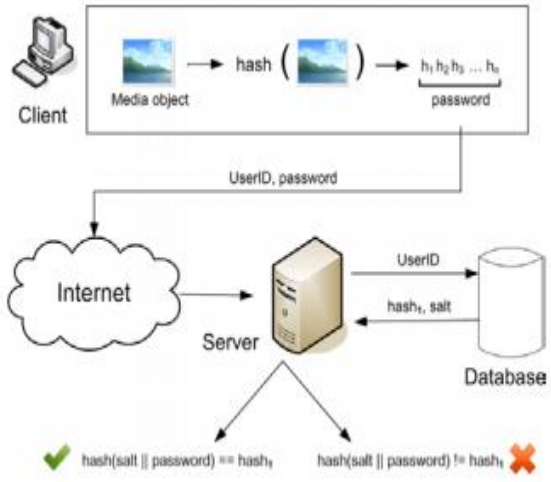

Fig. 2 Object Hash-Based Password Scheme.

The server-side implementation is identical to that of the text-based password scheme. The server receives the userID and a text-based version of the media object as opposed to the password in plaintext from the text-based scheme. However, since both of them are strings (character sequences), the subsequent computation is the same.

The client on the other hand requires some additional computation. A hash value (using SHA-256) is computed for the media object using a client-side script written in JavaScript.

The basic idea of this scheme is essentially the same as ObPwd. However, we use a stronger hash function i.e. SHA-256, instead of SHA-1 used in ObPwd. Further, ObPwd use PwdHash for reducing the hash values into a 12 characters long alphanumeric password and restricts the object size between 30 and 100000 bytes. Our solution does not apply any such restrictions.

OBJECT-BASED PASSWORD SCHEME

We extend the ObPwd scheme with a new object based password scheme that performs majority of the computation at the server side. This scheme extends the previous object hash-based scheme in such a way that majority of the computation is offloaded at the server side. In this scheme the media object selected by the user is directly sent to the server without any processing at the client side.

Fig. 3 highlights the differences of the object-based scheme with the text-based and the object hash-based schemes. When the digital object is transmitted, the server takes over the responsibility of computing the initial hash of the object. Once the text-based representation of the object is produced (i.e. the hash of the object), the server proceeds to validate authenticity of user based on the produced string.

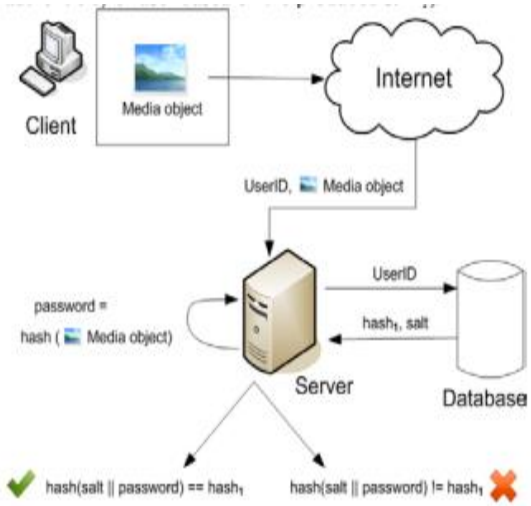

Fig. 3 Object-Based Password Scheme.

In this scheme the client is not required to perform any processing, and it is only responsible for uploading the media object to the server. Once the object is uploaded, a server-side script written in PHP computes the hash of the object using SHA-256, the produced hash we refer to as the password. As per the other schemes, the server retrieves the hash of the password and the salt from the data, re-hashes the password after concatenating it with the salt, and evaluates whether the user entered media object is valid. This scheme is beneficial when the client machine does not have sufficient processing power, for e.g. when the client is using a dumb terminal or a mobile device.

IV. CONCLUSION

The projected system provides safer student authentication system for on-line examination the item hash and object-based password schemes supply vital security edges over text-based password schemes if they're used properly. The selection between object hash and object based mostly password schemes may be a fairly easy one the item hash framework is a lot of economical in performance (similar to text-based schemes) however needs computation to be performed on the consumer. If that process power isn't accessible, then the item based mostly password theme is also the thanks to go even supposing it'll need considerably higher network resources and marginally higher server resources.

REFERENCES

[1] Kulvinder Kaur, Vineetha Khemchandani, Securing Visual Cryptographic Shares Using Public Key Encryption,3rd IEEE International Advance computing conference, 2013.

[2] Shyamalendu Kandar, Arnab Maiti," K-N secret sharing visual cryptography scheme for color image using Random number", vol 3, no.3, Mar 2011.

[3] InKoo Kang, Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Heung-Kyu Lee, Member, IEEE, "Color Extended Visual Cryptography Using Error Diffusion", IEEE Transactions on image processing, vol. 20, no. 1, January 2011.

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

[5] http://www.truecrypt.org/. Truecrypt.

[6] William Cheswick. Johnny can obfuscate: beyond mother's maiden name. In Proceedings of the 1st USENIX Workshop on Hot Topics in Security, HOTSEC'06, pages 6–6, Berkeley, CA, USA, 2006. USENIX Association.

[7] A. Houmansadr and S. Ghaemmaghami, "A novel video watermarking method using visual cryptography," in Proc. IEEE Int. Conf. Eng. Intell. Syst., 2006, pp. 1–5

[8] Manika Sharma, Rekha Saraswat ,Secure Visual Cryptography Technique for Color Images Using RSA Algorithm, International Journal of Engineering and Innovative Technology , Volume 2, Issue 10, April 2013

[9] Sonia Chiasson, Alain Forget, Elizabeth Stobert, P. C. van Oorschot, and Robert Biddle. Multiple password interference in text passwords and click-based graphical passwords. In Proceedings of the 16th ACM conference on Computer and communications security, CCS '09, pages 500–511, New York, NY, USA, 2009. ACM.

[10] Young-Chang Hou. Visual cryptography for color images. Pattern Recognition, 36:1619-1629, August 2002.

[11] Jim Cai, "A Short Survey On Visual Cryptography Schemes", 2004 http:// www.cs.toronto.edu/~jcai/paper.pdf.

[12] Ching-Nung Yang ,Tse-Slih Chen,"Colored Visual Cryptography Scheme based additive color mixing",Pattern Recognition,vol. 41,pp.3114- 3129,2008.

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

[14] Chin-Chen Chang, Jun-Chou Chuang, Pei-YuLin,"Sharing A Secret Two-Tone Image In Two GrayLevel Images", Proceedings of the 11th International Conference on Parallel and Distributed Systems.

[15] Katherine M. Everitt, Tanya Bragin, James Fogarty, and Tadayoshi Kohno. A comprehensive study of frequency, interference, and training of multiple graphical passwords. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '09, pages 889–898, New York, NY, USA, 2009. ACM.

[16] Dinei Florencio, Cormac Herley, and Baris Coskun. Do strong web passwords accomplish anything? In Proceedings of the 2nd USENIX workshop on Hot topics in security, HOTSEC'07, pages 10:1–10:6, Berkeley, CA, USA, 2007. USENIX Association.

[17] C.C. Wu, L.H. Chen, "A Study On Visual cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[18] H.-C.Hsu, T.-S. Chen,Y.-H.Lin, "The Ring Shadow Image Technology Of Visual Cryptography By Applying Diverse Rotating Angles To Hide The Secret Sharing", in Proceedings of the 2004 IEEE International Conferenceon Networking, Sensing & Control, Taipei, Taiwan, pp.996–1001, March2004.

[19] Marcia Gibson, Karen Renaud, Marc Conrad, and Carsten Maple. Musipass: authenticating me softly with ”my” song. In Proceedings of the 2009 workshop on New security paradigms workshop, NSPW ’09, pages 85–100, New York, NY, USA, 2009. ACM.

[20] Matt Weir, Sudhir Aggarwal, Michael Collins, and Henry Stern. Testing metrics for password creation policies by attacking large sets of revealed passwords. In Proceedings of the 17th ACM conference on Computer and communications security, CCS ’10, pages 162–175, New York, NY, USA, 2010. ACM.

[21] Sufian Hameed, S. A. Hussain and S. H. Ali, "SafePass: Authentication under duress for ATM transactions," In 2nd National Conference on Information Assurance (NCIA), 2013, pp. 1-5. doi: 10.1109/NCIA.2013.6725317.

[22] H.-C.Wu, C.-C.Chang, “Sharing Visual Multi-Secrets Using Circle Shares”, Comput. Stand. Interfaces 134 (28), pp.123–135, (2005)

[23] Chin-Chen Chang, Jun-Chou Chuang, Pei-YuLin, “Sharing A Secret Two-Tone Image In Two GrayLevel Images”, Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 2005.

[24] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, “Multiple-Image Encryption by Rotating Random Grids”, Eighth International Conference on Intelligent Systems Design and Applications, pp. 252-256, 2008.

[25] Reshma and Vijay Murari T.,”Survey on various visual cryptography techniques”.

[26] E. Verheuland H. V. Tilborg, “Constructions And Properties of K Out of N Visual Secret Sharing Schemes.”Designs, Codes and Cryptography, 11(2), pp.179–196, 1997.

[27] Liu, C.L. Introduction to Combinatorial Mathematics. McGraw-Hill, New York, 1968.

[28] Sagar Kumar Nerella, Kamalendra Verma Gadi and RajaSekhar Chaganti, “Securing Images Using Colour Visual Cryptography and Wavelets”, IEEE, vol.2 issue 3, March 2012.

[29] R. Biddle, M. Mannan, P. C. van Oorschot, and T. Whalen. User study, analysis, and usable security of passwords based on digital objects. Trans. Info. For. Sec., 6(3):970–979, September 2011.

[30] Mohammad Mannan and P. C. van Oorschot. Digital objects as passwords. In Proceedings of the 3rd conference on Hot topics in security, HOTSEC’08, pages 2:1–2:6, Berkeley, CA, USA, 2008. USENIX Association