IEAESP2018-141

Project Title : ENHANCED PASSWORD PROCESSING SCHEME BASED ON VISUAL CRYPTOGRAPHY AND OCR

Guide Details

Guide Name: Shashikala S V

Guide Email: Shashisv7@Gmail.Com

Guide Phone NO.: 9742084146

Qualification: M.Tech,(Phd)

Department: Computer Science And Engineering

Institute Name: BGS Institute Of Technology

College Address : B.G.Nagara,Bellur Cross

Students Details

Project Team Leader Name: Nandan B N

Email: Nandanbn996@Gmail.Com

Phone No. : 9886601383

Team Members list : Praveen Kumar, Priyadarshini B, Rakshitha B K

TITLE: ENHANCED PASSWORD PROCESSING SCHEME BASED ON VISUAL CRYPTOGRAPHY AND OCR

ABSTRACT

Traditional password conversion scheme for user authentication is to transform the passwords into hash values. These hash-based password schemes are comparatively simple and fast because those are based on text and famed cryptography. However, those can be exposed to cyber-attacks utilizing password by cracking tool or hash-cracking online sites. Attackers can thoroughly figure out an original password from hash value when that is relatively simple and plain. As a result, many hacking accidents have been happened predominantly in systems adopting those hash-based schemes. In this work, we suggest enhanced password processing scheme based on image using visual cryptography (VC). Different from the traditional scheme based on hash and text, our scheme transforms a user ID of text type to two images encrypted by VC.

The user should make two images consisted of subpixels by random function with SEED which includes personal information. The server only has user's ID and one of the images instead of password. When the user logs in and sends another image, the server can extract ID by utilizing OCR (Optical Character Recognition). As a result, it can authenticate user by comparing extracted ID with the saved one. Our proposal has lower computation, prevents cyber-attack aimed at hashcracking, and supports authentication not to expose personal information such as ID to attackers.

INTRODUCTION

User authentication in general systems has proceeded basically through verification of the ID and password. In order to send and verify password, the system uses a hash-based password scheme that transforms original password to hash value by famed function. The advantages are that it can be adapted in system without difficulty, and computational velocity of process is fast because a type of hash-based scheme is fundamentally based on text utilizing popular hash function such as MD5, SHA256. But it is vulnerable to attacks such as brute force attack or dictionary-based attack plainly by password cracking tool or hash-cracking online sites. Assume that someone defines password “1qaz2wsx” in a system. If an attacker is aware of the hash value “1c63129ae9db9c60c3e8aa94d3e00495”, the value can be sufficiently cracked simply by free crack site. Even though the attacker doesn’t know any information about hash function, he or she can easily guess which kind of hash function is adapted in the system. As the result, the attacker can cause secondary damage to the system.

LITRATURE SURVEY

Gaw, Shirley, and Edward W. Felten, "Password management strategies for online accounts," Proceedings of the second symposium on Usable privacy and security. ACM, 2006
Given the widespread use of password authentication in online correspondence, subscription services, and shopping, there is growing concern about identity theft. When people reuse their passwords across multiple accounts, they increase their vulnerability; compromising one password can help an attacker take over several accounts. Our study of 49 undergraduates quantifies how many passwords they had and how often they reused these passwords. The majority of users had three or fewer passwords and passwords were reused twice. Furthermore, over time, password reuse rates increased because people accumulated more accounts but did not create more passwords. Users justified their habits. While they wanted to protect financial data and personal communication, reusing passwords made passwords easier to manage. Users visualized threats from human attackers, particularly viewing those close to them as the most motivated and able attackers; however, participants did not separate the human attackers from their potentially automated tools. They sometimes failed to realize that personalized passwords such as phone numbers can be cracked given a large enough dictionary and enough tries. We discuss how current systems support poor password practices. We also present potential changes in website authentication systems and password managers.

Tam, Leona, Myron Glassman, and Mark Vandenwauver, "The psychology of password management: a tradeoff between security and convenience, "Behaviour& Information Technology 29.3 (2010): 233- 244.
Despite technological advances, humans remain the weakest link in Internet security. In this study, we examined five password-management behaviours to answer questions about user knowledge of password quality, motivation behind password selection and the effect of account type on password-management behaviour. First, we found that users know what constitutes a good/bad password and know which common password-management practices are (in)appropriate. Second, users are motivated to engage in these bad password-management behaviours because they do not see any immediate negative consequences to themselves (negative externalities) and because of

the convenience–security tradeoff. Applying Construal Level Theory, we found that this tradeoff can be positively influenced by imposing a time frame factor, i.e. whether the password change will take place immediately (which results in weaker passwords) or in the future (which results in stronger passwords). Third, we found a time frame effect only for more important (online banking) accounts.

Dana Yang, InshilDoh, KijoonChae, "Mutual Authentication based on Visual Cryptography and OCR for Secure IoT Service," Source of the Document 2016 6th International Workshop on Computer Science and Engineering.

Traditional password conversion scheme for user authentication is to transform the passwords into hash values. These hash-based password schemes are comparatively simple and fast because those are based on text and famed cryptography. However, those can be exposed to cyber-attacks utilizing password by cracking tool or hash-cracking online sites. Attackers can thoroughly figure out an original password from hash value when that is relatively simple and plain. As a result, many hacking accidents have been happened predominantly in systems adopting those hash-based schemes. In this work, we suggest enhanced password processing scheme based on image using visual cryptography (VC). Different from the traditional scheme based on hash and text, our scheme transforms a user ID of text type to two images encrypted by VC. The user should make two images consisted of subpixels by random function with SEED which includes personal information. The server only has user's ID and one of the images instead of password. When the user logs in and sends another image, the server can extract ID by utilizing OCR (Optical Character Recognition). As a result, it can authenticate user by comparing extracted ID with the saved one. Our proposal has lower computation, prevents cyber-attack aimed at hash-cracking, and supports authentication not to expose personal information such as ID to attackers.

Naor and A. Shamir, "Visual Cryptography," Advances in Cryptology EUROCRYPT94 LNCS, Vol. 950, pp. 1-12, 1995.

In this paper we consider a new type of cryptographic scheme, which can decode concealed images without any cryptographic computations. The scheme is perfectly secure and very easy to implement. We extend it into a visual variant of the *k* out of *n* secret sharing problem, in which a dealer provides a transparency to each one of the *n* users; any *k* of them can see the image by stacking their transparencies, but any *k*−1 of them gain no information about it.

Gauravaram, Praveen, "Security Analysis of salt|| password Hashes," Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on. IEEE, 2012.

Protection of passwords used to authenticate computer systems and networks is one of the most important application of cryptographic hash functions. Due to the application of precomputed memory look up attacks such as birthday and dictionary attacks on the hash values of passwords to find passwords, it is usually recommended to apply hash function to the combination of both the salt and password, denoted salt||password, to prevent these attacks. In this paper, we present the first security analysis of salt||password hashing application. We show that when hash functions based on the compression functions with easily found fixed points are used to compute the salt||password hashes, these hashes are susceptible to precomputed offline birthday attacks. For example, this attack is applicable to the salt||password hashes computed using the standard hash functions such as MD5, SHA-1, SHA-256 and SHA-512 that are based on the popular Davies-Meyer compression function. This attack exposes a subtle property of this application that although the provision of salt prevents an attacker from finding passwords, salts prefixed to the passwords do not prevent an attacker from doing a precomputed birthday attack to forge an unknown password. In this forgery attack, we demonstrate the possibility of building multiple passwords for an unknown password for the same hash value and salt. Interestingly, password||salt (i.e. salts suffixed to the passwords) hashes computed using Davies-Meyer hash functions are not susceptible to this attack, showing the first security gap between the prefix-salt and suffix-salt methods of hashing passwords.

TOOLS

HARDWARE REQUIREMENTS:

• **System**	:	Pentium IV 2.4 GHz.
• **Hard Disk**	:	500 GB.
• **RAM**	:	4 GB

Any desktop / Laptop system with above configuration or higher level

SOFTWARE REQUIREMENTS:

Operating system	:	Windows XP / 7
Coding Language	:	Java (Jdk 1.7)
Web Technology	:	Servlet, JSP
Web Server	:	TomCAT 7.0
IDE	:	Eclipse Galileo
Database	:	My-SQL 5.0
UGI for DB	:	SQLyog
JDBC Connection	:	Type 4 - Native Drive

METHODOLOGY

- Visual Cryptography
- OCR algorithm

PROBLEM STATEMENT

Even though the attacker doesn’t know any information about hash function, he or she can easily guess which kind of hash function is adapted in the system. As the result, the attacker can cause secondary damage to the system. Participants have the responsibility on this kind of attacks. When a researcher inquired to many people about password management behavior

PROPOSED SYSTEM

The user inputs the ID and password. The device of user creates an original image composed of black characters and white background. If the saved original image exists on user’s device, it does not have to create the original image again. Although the device does not possess the first shared image, it can thoroughly construct second shared image referred to the original image and first shared image because the device already knows the SEED to make up the first shared image.

The user sends the second shared image only to the server. The server overlaps the first shared image saved and the second shared image received.The server should remove the background of the overlapped image as in Figure 3 (d), to gain original image.ID is retrieved from the background-removed image by OCR.The server confirms whether the extracted ID corresponds with saved ID, and determines success or fail.Finally result is sent to the user.

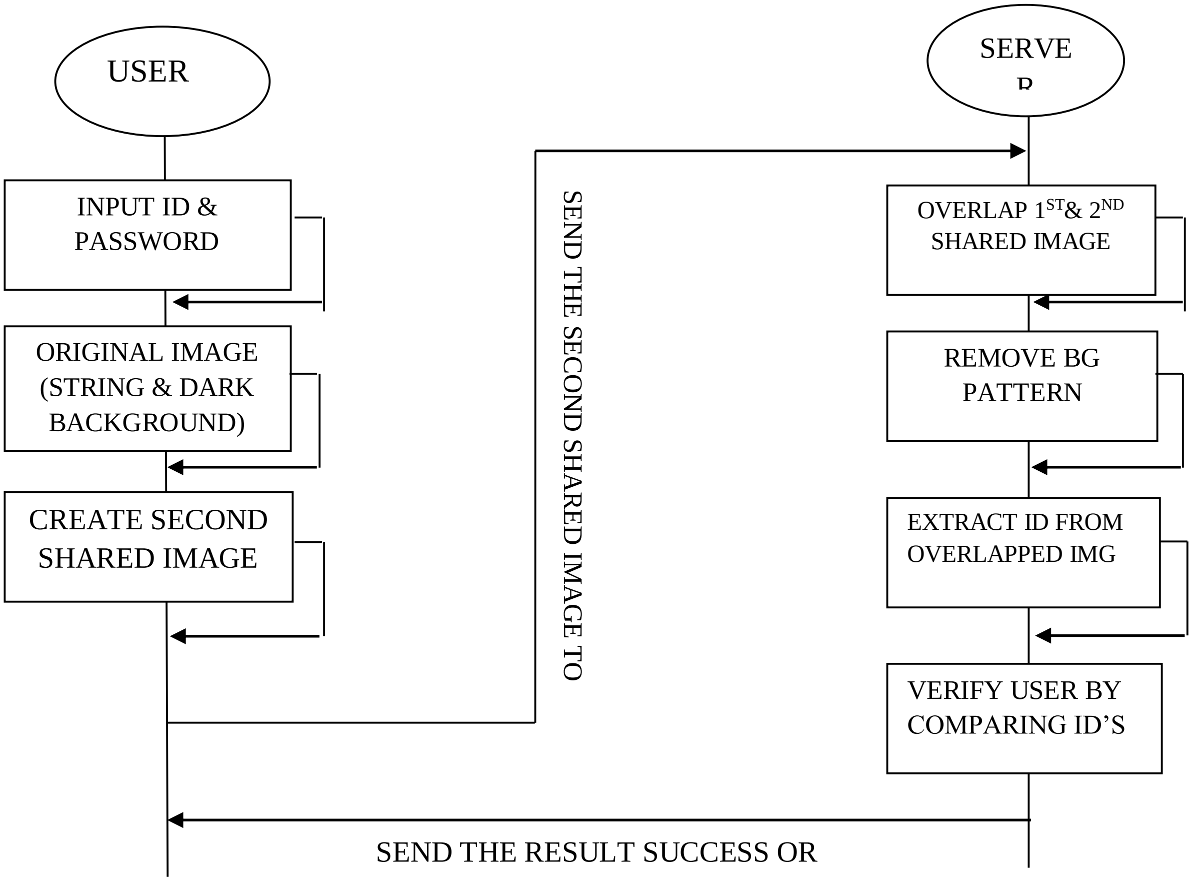
USER
INPUT ID & PASSWORD
ORIGINAL IMAGE (STRING & DARK BACKGROUND)
CREATE SECOND SHARED IMAGE
SEND THE SECOND SHARED IMAGE TO
SERVE R
OVERLAP 1ST& 2ND SHARED IMAGE
REMOVE BG PATTERN
EXTRACT ID FROM OVERLAPPED IMG
VERIFY USER BY COMPARING ID'S
SEND THE RESULT SUCCESS OR

FIG 1: PROCESS OF ENHANCED PASSWORD SCHEME

ADVANTAGES

The goal of our proposal is to prevent cyber-attack and support privacy of personal information.

CONCLUSION

Our proposal has lower computation, prevents cyber-attack aimed at hash cracking, and supports authentication not to expose personal information such as ID to attackers.

BASE PAPER

Enhanced Password Processing Scheme Based on Visual Cryptography and OCR by Dana Yang, Inshil Doh & Kijoon Chae, Ewha Womans University, Seoul, Korea.(IEEE 2017)

OTHER REFERENCES

[1] Gaw, Shirley, and Edward W. Felten, "Password management strategiesfor online accounts," Proceedings of the second symposium on Usableprivacy and security. ACM, 2006.

[2] Nguyen, Thi Thu Trang, and Quang Uy Nguyen, "An analysis ofPersuasive Text Passwords, "Information and Computer Science (NICS),2015 2nd National Foundation for Science and Technology DevelopmentConference on. IEEE, 2015.

[3] Tam, Leona, Myron Glassman, and Mark Vandenwauver, "Thepsychology of password management: a tradeoff between security andconvenience, "Behaviour & Information Technology 29.3 (2010): 233-244.

[4] Wang, Luren, Yue Li, and Kun Sun, "Amnesia: A Bilateral GenerativePassword Manager," 2016 IEEE 36th International Conference onDistributed Computing Systems

[5] Gauravaram, Praveen, "Security Analysis of salt|| password Hashes,"Advanced Computer Science Applications and Technologies (ACSAT),2012 International Conference on. IEEE, 2012.

[6] Dana Yang, Inshil Doh, Kijoon Chae, “Mutual Authentication based onVisual Cryptography and OCR for Secure IoT Service,” Source of theDocument 2016 6th International Workshop on Computer Science andEngineering, WCSE 2016, 2016, Pages 214-219

[7] M. Naor and A. Shamir, “Visual Cryptography,” Advances in CryptologyEUROCRYPT94 LNCS, Vol. 950, pp. 1-12, 1995.

[8] Mori, Shunji, Ching Y. Suen, and Kazuhiko Yamamoto, "Historicalreview of OCR research and development," Proceedings of the IEEE 80.7(1992): 1029-1058.

[9] Patel, Chirag, Atul Patel, and Dharmendra Patel, "Optical characterrecognition by open source OCR tool tesseract: A case study,"International Journal of Computer Applications 55.10 (2012).

[10] Holley, Rose, "How good can it get? Analysing and improving OCRaccuracy in large scale historic newspaper digitisation programs," D-LibMagazine 15.3/4 (2009).

[11] Marsaglia, George, "Xorshift rngs," Journal of Statistical Software 8.14(2003): 1-6.