Australian Journal of Basic and Applied Sciences, 7(4): 415-418, 2013
ISSN 1991-8178

Access Control Based on Pixel Value Extraction

Mohd Afizi Mohd Shukran, Mohd Sidek Fadhil Mohd Yunus, Kamaruzaman Maskat

Faculty of Defense Science and Technology, Universiti Pertahanan Nasional Malaysia (UPNM), Kem Sungai Besi, 57000 Kuala Lumpur, Malaysia

Abstract: This paper is to introduce a new access control method based on image file's pixel value. The method is aim to be invincible from key-logger software. Key-logger is a spy-ware that resides in a workstation to log every key-stroke, and the key-stroke logs are accessible through remote location. Key-logger is able to get every single character typed-in in plain-text. Passwords that should be confidential are readable easily when the key-stroke logs being retrieve by hacker. Pixel Value user access control method is not involving password key-in on a workstation. The password has been stored in server and it is a pixel value generated from extracted image file through image compression algorithm, in example Discrete Cosine Transform (DCT). Image compression algorithm is a series of mathematical functions that calculate color composition on single image file and usually used to authenticate watermarking on image. The algorithm produces pixel value that used as password to authenticate a user access. It is secretly kept on database and even users have no idea what is the password. User only need to upload their security image, so called *passpict* in order to log-in. Pixel Value user access control can be suitable to implement on web-based application log-in such as web-mail, social network, online portal, and banking portal.

Key words: Pixel Value, Image Compression Algorithm, Authentication, Log-in, Passpict,

INTRODUCTION

Pixel value access control is a method to provide a new secure guard mechanism for access control on online or any web based system. It is a way to avoid end user to key-in their password being capture by key-logger software. With an pixel value access control guarded system, an image will be used to authenticate their identity; it is so call *Passpict* rather than password as authentication. The end-user required to upload their known image in order to log in to an online system. When the server receives the *passpict*, the system will extract pixel value from the picture and used its value as authentication value for respective user-name. The way to extract pixel value from an image is using Image compression techniques. There are various imaging compression algorithms and each compression techniques produce an output in quantitative value or known as pixels value. The pixels value will be used to authenticate a user-name. The end users are authenticated and authorized to access their resource on the network without entering passwords. Key-logger software got no keystroke capture, and the end-user account is safe.

Through this paper, pixel value concept and its process are briefly explained in section 1.1, pixel value. Section 2 of this paper listed some related image authentication or graphical password design and implementation. On section 3, proposed method, discuss on current implementation problem and proposed solution design. Conclusion and significant of this method will discuss on section 4

1.1 Pixel Value:

Each digital image files stored inside a computer has a pixel value which describes how bright that pixel is, and what color it should be. The most common pixel format is the byte image, where this number is stored as an 8-bit integer giving a range of possible values from 0 to 255. Typically zero is taken to be black, and 255 are taken to be white. During extraction through certain algorithm, the image files are dividing into grids; it can be 8 by 8 grid or 16 by 16 grids. Each grid is being calculated its pixel value with compression algorithm. Then, all grids' pixel value will be transform into a single value with compression algorithm once again. This is how pixel value is being produce and acquire from an image. In this authentication method, pixel value will be used as authentication key for a user-name.

2. Related Works:

In the United State of America, a lot of image based access control patents publication has been issued such as U.S. Patent No. 5,559,961 by Blonder, U.S. Patent Application Publication No. 2003/0191947 to

Corresponding Author: Mohd Afizi Mohd Shukran, Faculty of Defense Science and Technology, Universiti Pertahanan Nasional Malaysia (UPNM), Kem Sungai Besi, 57000 Kuala Lumpur, Malaysia
E-mail: afizi@upnm.edu.my

Stubblefield, and U.S. Patent Application Publication No. 2004/0230843 to Jansen. Based on these patents image based access control is applied for double layer protection for current log-in guard system. (User-name and password). When a user's user-name and password has been authenticate, user need to choose a image from the server library in order to proceed to their account. The image set has been provided by server and users need to choose from library collection. A single image can be used by multiple users by its default design. This design is known as graphical password.

Graphical password for access control was implemented by MAYBANK. It has similarity with design that patent in U.S.A. MAYBANK, a Malaysians banking and financial institution, with their Online Banking service called Maybank2u.com, the client needs to select an image icon with their challenge phrase under that image that they selected. Now the user will save additional information to the Maybank2u.com server. This image with its challenge phrase will appear each and every time before a user specify their password for log-in. The reason of this feature added, is to ensure that the bank knows something that the user know.

Image Compression Techniques has been widely used for image authentication to determine watermarking on a single digital image file. Most picked compressions techniques are Discrete Cosine Transform and Wavelet Transform. Digital Watermarking purpose was for protecting digital imaging copyright and originality. In watermarking authentication, the picture will be extract into pixel value to find hiding pattern on image. Based on acquired pixel value, the brightness and darkness of each grid will determine watermarking pattern on image. Many techniques has been developed and applied for watermarking authentication purpose.

3. Propose Method:

Based on current implementation, the image that used to authenticate a user has been provided and it is common image libraries such as cartoon dinosaurs, dogs, and cars. In other words, the image libraries are viewable and exposed to everyone. With high intention of breaking into a user account, the security parameter can be by-pass by traditionally choose each available image on library properly. After a series of worth trying, hackers are successfully breaking into an account. Theoretically, image brute-force tools can bypass this authentication system. Image brute-force tools attempt to find the correct image by scanning each image grid.

For traditional log-in page, users require to key-in user-name and password. A hidden Key-logger will capture the actual user-name and password on an end-user workstation. The confidentiality of a password easily leaked not just through key-logger software, password can be easily obtained through simple spying techniques, shoulder suffer, as a person with malicious intent simply look the log-in or through private conversation eavesdropping.

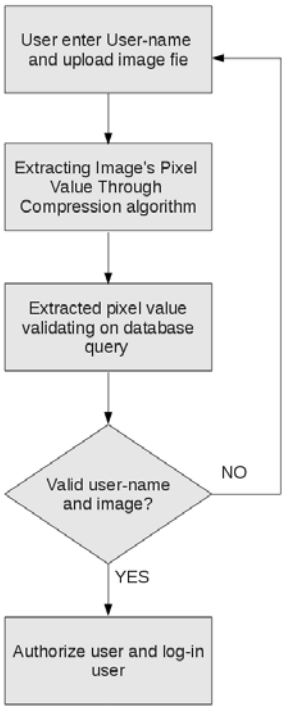

Fig. 1: Log-in process for Pixel Value User Access Control.

This proposed method is involving image as key-pass for a log-in system. Based on user-name - password concept and graphical password concept, pixel value user access control is combination of both concepts. With pixel value user access control method, users just need to enter user-name and upload their security image to the log-in page. The security image is just known by the user secretly, so called as *passpict*, and not keep on server. Server then, extract the uploaded image to get its' pixel value that will be used to authenticate a user. The pixel value is bringing to query for next authentication process. User-name and pixel value are being validate from user database. The user will grant for access if the user-name and pixel value is successfully passing the validating process. The user account details are storing in a database that containing user-name and pixel value.

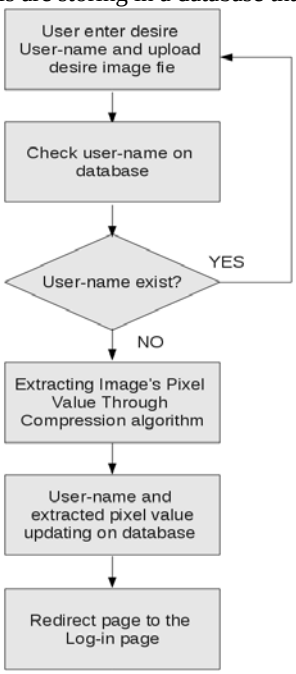

Fig. 2: User enrollment process for pixel value user authentication.

In order to enable or activate a user-name on log-in, users have to register their user-name and image file. This process require user to key in their user-name and upload their *passpict* as prerequisite for system. Other details such as full name will be just for system records. System itself will find user-name record for any existing user-name. If the user-name has been registered and existed on database, user need to chose another user-name and refill on enrollment page. For a newly register 'user-name, system will extract the uploaded image file to acquire its' pixel value through image compression algorithm. User-name, pixel value, and other records are being inserted into database. Enrolled user-name and image's pixel value are ready to being used on log-in page.

Through pixel value user authentication method, user themselves have no information or idea what is the plain-text of their password since it is keep in their *passpict* file. It is end user responsibility to keep the *passpict* safely from being use for identity theft. User may use a usual image file as *passpict* such as social network site profile picture, company logo, and image on personal blog, and any image file stored in USB drive, but no one should know it is a *passpict* file. User may keep their *passpict* on any digital space locally or online as long as it is reachable when it is needed.

4. Conclusion:

User access control based on pixel value is a hybrid log-in method from user-name – password concept and graphical password concept. Unlike current implementation, where user needs to pick a image from listed image libraries, this method will give user flexibility to use their own meaningful security image as their authentication parameters or *passpict*. Plus, it is easy to remember their own meaningful image rather than they need to choose image that meaningless to them. Hackers have no idea what image that user being use as *passpict* when it is securely kept by user. As traditional passwords, where user needs to renew their password periodically, *passpict* might be change by user as *Facebook* profile picture.

This authentication method brings a lot of benefits which is:

- When a key pass transfer across the network without using conventional text format make cracking tools and method are unable to define the password.
- Key logger is unable to capture typing text when there is no password key in involving.
- Using image identification, much more easily to memorize than word phrase. Forgotten password issue will be reduce
- Upload module are replacing password text box will protect login page from brute force attack or dictionary attack.

ACKNOWLEDGEMENTS

This research was supported by the Ministry of Higher Education of under grant *RESEARCH ACCULTURATION COLLABORATIVE EFFORT (RACE)*, 2012.

REFERENCES

Fisher, R., S. Perkins, A. Walker and E. Wolfart, 2003. Pixel Value, Retrieved on 21 December 2011, From http://homepages.inf.ed.ac.uk/rbf/HIPR2/value.htm.

Graves, Kimberly, 2010. CEH Certified Ethical Hacker Study Guide, John Wiley & Sons, Incorporated.

Malayan Banking Berhad press release, 2011. Maybank2u.com introduce additional security features. Retrieved July 5, 2011 from http://www.maybank.com.my/corporate-profile/corporate-news/maybank2ucom-introduces-additional-security-features.

Mona F.M. Mursi, Ghazy M.R. Assassa, Hatim A. Aboalsamh, Khaled Alghathbar, 2009. A DCT - Based Secure JPEG Image Authentication Scheme. World Academy Of Science, Engineering and Technology, 682-687.

Sumo Brain Solution, 2012. Graphical Image Authentication And Security System. Retrieved on 15 February 2012, From http://www.freepatentsonline.com/y2012/0023574.html.

United States Patent Application Publication, 2012. Graphical Image Authentication And Security System (Publication No. US 2012/0023574 A1). Portland, Orlando.