Cloud Publications
International Journal of Advanced Computer Science and Information Technology
2013, Volume 2, Issue 1, pp. 29-33, Article ID Tech-68
ISSN 2320 – 0235

Review Article | Open Access

Password Authentication System (PAS) for Cloud Environment

Bhavana A., Alekhya V., Deepak K., and Sreenivas V.

Department of C.S.E., K L University, Vaddeswaram, Guntur, Andhra Pradesh, India

Correspondence should be addressed to Bhavana A., bhavana@kluniversity.in

Publication Date: 5 April 2013

Article Link: http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-68

Abstract Verification is the major part of protection against compromising secrecy and authenticity. Though long-established login/password based schemes are easy to implement in the cloud environment, they have been subjected to numerous attacks. As a substitute, token and biometric based verification systems were introduced for security. However, they have not enhanced significantly to justify the expenditure. For providing more security-in this paper, we introduce a new framework i.e., Password Authentication System for Cloud Environment (PASCE), which is immune to the common attacks suffered by other verification schemes.
Keywords *Password Authentication System, Cloud Computing, Smartcards*

1. Introduction

Because of emergent threats to networked computer systems, there is great need for security innovations. Security practitioners and researchers have made strides in defending systems and, correspondingly, individual users' digital possessions. However, the difficulty arises that, until recently, security was treated completely as a technical problem- the system user was not factored into the equation. Users interact with protection technologies either passively or actively. For passive use understandability may be enough for users. For active use people need much more from their security solutions: ease of use, exorability, competence and satisfaction [5]. Today there is an increasing detection that security issues are also basically human computer interaction issues. Validation is the process of determining whether a user should be allowed access to a particular system or resource. It is a critical area of security research and practice. Alphanumeric passwords [4] are used widely for verification, but other methods are also available today, as well as biometrics and smart cards. However, there are problems of these substitute technologies. Biometrics raise confidentiality concerns and smart cards usually need a PIN because cards can be lost [6]. As a result, passwords are still leading and are expected to continue to remain so for some time. Yet conventional alphanumeric passwords have drawbacks from a usability standpoint, and these usability problems tend to transform directly into security problems. That is, users who fail to choose and handle passwords securely open holes that attackers can utilize.

2. Cloud Computing

Cloud computing gets its name as a symbol for the Internet. Typically, the Internet is represented in network diagrams as a cloud. Cloud computing promises to cut operational and capital costs and, more importantly, Cloud technology provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services [11]. Cloud computing [11] is distributed processing, parallel processing and the development of grid computing, or commercial implementations of these concepts of computer science. In the cloud computing model is the essential structure of which, the foundation part is collected of more than one computer server "cloud." It gathers all the resources together to form large data storage and processing center. Let IT departments focus on intentional projects instead of keeping the datacenter running. Cloud computing provides the most consistent and secure data storage center. Users do not have to worry about data loss, virus attack and other problems. The "cloud" manages information by a professional team. Besides, strict rights management strategy can help to share data.

3. Introduction for Authentication

There are numerous validation schemes existing in the literature. They can be broadly classified as follows:

- What you know
- What you have and
- What you are

The conventional username/password or PIN based certification scheme is an example of the "what you know type". Smartcards or electronic tokens are examples of "what you have type of authentication" and finally biometric based certification schemes are examples of the "what you are" type of validation. Some validation systems may use an arrangement of the above schemes. In This paper, we focus only on "what you know" types of validation. Although traditional alphanumeric passwords are used widely, they have problems such as being hard to memorize, vulnerable to guessing, dictionary attack, key-logger, Shoulder-surfing and social engineering. In addition to these types of attacks, a user may tend to choose a weak password or record his password. This may further decline the validation schemes. As an alternative to the conventional password based scheme, the biometric system was introduced. This relies upon exclusive features unchanged during the life time of a human, such as finger prints, iris etc. The major problem of biometric as a validation scheme is the high cost of additional devices needed for recognition process. The false-positive and false negative rate may also be high if the devices are not robust. Biometric systems are bare to replay attack (by the use of close excess left by finger on the devices) [3], which decrease the security and usability levels. Thus, modern developments have attempted to defeat biometric shortcomings by introducing token-based authentication schemes. Token based systems rely on the use of a physical device such as smartcards or electronic-key for validation purpose. This may also be used in conjunction with the conventional password based system. Token based systems are vulnerable to man-in-the middle attacks where an intruder intercepts the user's session and records the credentials by acting as a proxy between the user and the authentication device without the knowledge of the user. Thus as an unusual, graphical based passwords are introduced to resolve security and usability restrictions mentioned in the above schemes. Graphical-based password techniques have been proposed as a potential alternative to text-based techniques, supported partially by the fact that humans can remember images better than text. Psychologists have confirmed that in both detection and recall scenarios, images are more memorable than text. Therefore, graphical-based proof schemes have higher usability than other validation techniques. On the other hand, it is also complex to break graphical passwords using normal attacks such as dictionary attack, brute force and spyware

which have been affecting text-based and token-based authentication. Thus, the security level of graphical based validation schemes is higher than other authentication techniques.

In broad-spectrum, the graphical password techniques can be classified into two categories:

1. Recognition-based graphical technique.
2. Recall based graphical technique.

A. Recognition-Based Systems

In recognition-based systems, a cluster of images are display to the user and a usual validation requires a correct image being touched in an exacting order. Some examples of recognition-based system are IAS system [2], reliable Graph, and Pass faces system [4]. An image password called IAS [2] is a new system which enables users to use their preferred image instead of a text password for validation purpose. Even though PAS system has a superior usability, it is difficult to execute due to the storage space needed for images and also the system cannot stand replay attack.

Image Authentication System (IAS): Image-based Authentication with Image Registration and Notification Interfaces

IAS is a validation system using photographs as a substitute of passwords. It, Moreover, integrates image check and notification interfaces into current validation frameworks (Figure 1). The image muster line enables users to add their preferred images to the validation system. As a result, this makes it possible for users to use their preferred image as a “pass-image”. Almost 20 million users currently have mobile phones with digital cameras in Japan. Most of them send photos by E-mail with a few key clicks on the spot. The image muster interface is implemented using this function. It is implemented independently from a pass-image [2] setting in order to ensure the privacy against copying attempts. This task simply enables users to add a photo to the system and a registered photo does not automatically become a pass-image. In other words, not all registered images become a passim age. A user must set at least one pass-image before authenticating oneself using IAS.

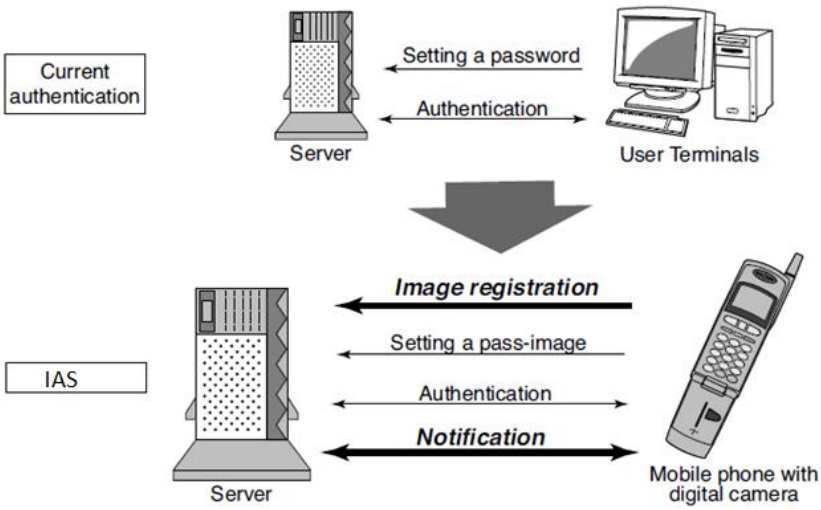

Figure 1: *Transition between Current and Proposed Authentication Framework [2] Takada.T and H. Koike*
Source: This image has taken from the paper entitled Awase-E: Image-based authentication for mobile phones using user's favorite images authored by Takada.T and H. Koike

The warning interface gives users activate to handle a risk sensibly. It notifies users of the incidence of all kinds of events related to the validation process. For example, IAS sends an E-mail to the user who has registered a photo. The E-mail has a URL. The web page that is linked by that URL contains the photo that a user has just registered. A user can thus confirm the registered photo immediately through a web page. If a user receives such an E-mail even though the user had not registered the photo, it means that someone has registered it unknown as a legitimate user. A reasonable user, therefore, quickly knows when an invasive attempt has been made. From these scenarios, we would stoutly recommend using IAS with mobile phones to ensure a user's rapid awareness of a security breach. IAS keeps an event history of past usage for certain periods for the purpose of auditing the user's validation usage. A user can investigate the history through a web page. It enables users to check the authentication usage even if a user has lost their mobile phone.

IAS is implemented through both E-mail and Web. Prerequisite supplies for a user terminal are that it has access to the above two network service types. This means that it is also possible to use IAS from computers. The detail of the validation process is shown in Figure 2.

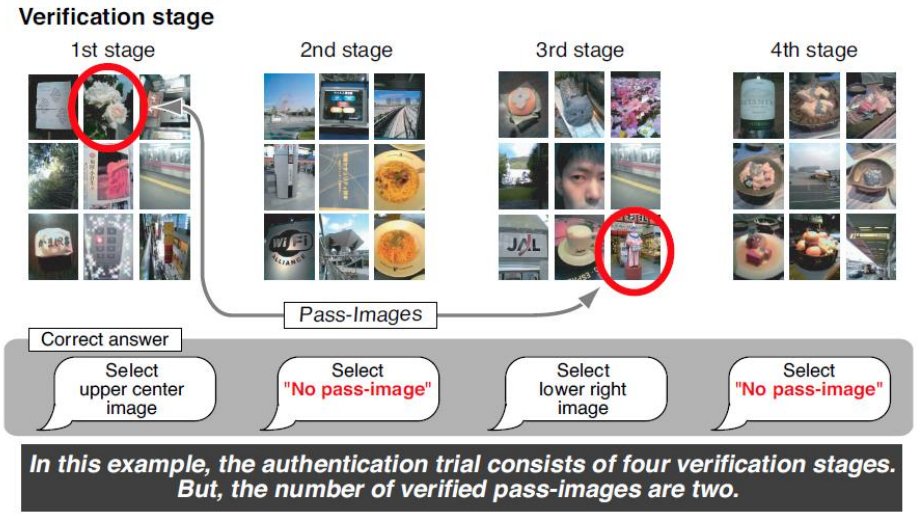

Figure 2: *A Detailed Authentication Process in PAS (N=4, P=9) [2] Takada.Tand H. Koike*
Source: This image has taken from the paper entitled Awase-E: Image-based authentication for mobile phones using user's favorite images authored by Takada.T and H. Koike

One verification test consists of R times of qualifications stages. IAS, of course, authorizes a user as genuine user only if all verifications are successful. In each verification stage, IAS shows X pieces of images on the screen, a user must select a pass-image correctly from them. Only one pass image is built-in in each verification image set. The motive for this is to decrease the possibility that an accidentally selected attacker's answer would be a correct answer. We call an image that is not a pass-image as a "decoy image". The position of each image in the image set is randomly determined. This means that the location of both pass-image and decoy images can change each time. It is also possible that there is no pass image in an image set. In this case, the user must answer "no pass-image". IAS is an easier method for users to complete the validation process than before, even when using a mobile phone. The arithmetical keys on a mobile phone are uniquely corresponding to each of the images on the screen at any given stage. This enables users to decide any image in the screen with one click. In using IAS, it is possible to substantiate oneself by just N + 2 times of key types.

Additionally, IAS does not need to input any text in validate oneself because it uses an E-mail address as a user ID.

B. Recall-Based Systems

In recall-based systems, the user is asked to replicate something that he/she created or selected former during the registration phase.

Password Authentication System for Cloud Environment (PASCE)

Graphical authentication system with image reshuffle format is given for the cloud environment when the data upload/download into the cloud account.

4. Conclusion

In this paper, we have proposed a new Password Authentication System for Cloud Environment where the verification information is absolutely accessible to the user. If the user "clicks" the image for verification and it compared with the server, the user is implicitly genuine. No password information is exchanged between the client and the server by using PAS authentication system. Since the authentication information is conveyed absolutely. Strength of PASCE lies in creating a good verification space with adequately huge set of images to shun short repeating cycles.

References

[1] Susan Wiedenbeck et al., 2005: *Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice*. Symposium on Usable Privacy and Security (SOUPS) Pittsburgh, PA, USA.

[2] Takada T., et al. *Awase-E: Image-Based Authentication for Mobile Phones Using User's Favorite Images*. Human-Computer Interaction with Mobile Devices and Services, Springer Berlin/ Heidelberg. 2003. 2795; 347-351.

[3] Dhamija R., et al., 2000: *A User Study Using Images for Authentication*. 9th Usenix Security Symposium, Denver, Colorado, 45-58.

[4] Suo X., et al., 2005: *Graphical Passwords: A Survey*. Computer Security Applications Conference, 21st Annual, Tucson, AZ, 472.

[5] Wu C.W. *On the Design of Content-Based Multimedia Authentication Systems*. IEEE Trans. Multimedia.2002. 4 (3) 385-393.

[6] R. Morris et al. *Password Security: A Case History*. Commun. ACM. 1979. 22; 594-597.

[7] Birget J.C., 2003: *Robust Discretization: With an Application to Graphical Passwords*. Cryptology ePrint Archive, Report 2003/168.

[8] Renaud K. *On User Involvement In Production of Images Used in Visual Authentication*. J. Vis. Lang. Comput. 2009. 20 (1) 1-15.

[9] Wiedenbeck S., et al., 2005: *Authentication Using Graphical Passwords: Effects of Tolerance And Image Choice.* Symposioum. Usable Privacy and Security, Carnegie-Mellon Univ., Pittsburgh, PA.

[10] Blonder G., 1996: *Graphical Password*. U.S. Patent 5 559 961.

[11] Sreenivas V., et al. *Efficient Use of Cloud Computing in Medical Science*. American Journal of Computational Mathematics. 2012. 2; 240-243.