Research Article Impact Factor: 4.226 ISSN: 2319-507X
Ritika Sachdev, IJPRET, 2014; Volume 3 (1): 77-84 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

USER AUTHENTICATION: A CASE HISTORY

RITIKA SACHDEV
Department of Computer Science, Smt. Chandibai Himathmal Mansukhani College, Ulhasnagar,

Accepted Date: 16/08/2014; Published Date: 01/09/2014

Abstract: In this paper, a comparative study of software-based user authentication techniques, and also the use of traditional password techniques and PINs against numerous alternative methods involving graphical password schemes is made. In order to achieve authentication, all these methods depend upon the user‟s ability to recall some secret knowledge which forms the basis of these methods. Moderately comprehensive overview of various researchers‟ work in this regard, covering both usability and security aspects is then presented, highlighting novel features thereof. Keeping in mind, the security threats that various graphical or otherwise password schemes may suffer from, attention is drawn to the latest attempts which include odour based password, pass films and demographic maps.

Keywords: Authentication, Cognometrics, Tokens, Biometrics, Graphical Password, Filmpw, Scent Signature

Corresponding Author: MS. RITIKA SACHDEV

Access Online On:

www.ijpret.com

How to Cite This Article:

Ritika Sachdev, IJPRET, 2014; Volume 3 (1): 77-84

PAPER-QR CODE

INTRODUCTION

In our present day-today living, it is very often that we need to authenticate ourselves on various information systems. In this context, user authentication simply means the act of confirmation of the user‟s claimed digital identity. “Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be” [1].

Traditionally, such authentication mechanisms are classified into three types, each having its own pros and cons.

Cognometrics: (kagnωɛmɛtriks) [sic] 1. n. a measurable, innate cognitive ability of the human brain (e.g. ability to recognize a familiar face or musical tune). 2. n. method of personal authentication based on measuring an innate cognitive ability of the human brain (e.g. ability to recognize a familiar face) [2]. (Latin: cognoscere – to learn, Greek: metron – to measure). This category of authentication mechanism comes under “something the user knows”. Relevant examples of this popular and widespread category are passwords and PINs. The mechanism owes its popularity as the stakeholders do not require any additional training in using it neither any special hardware is required to implement it. Cognometrics are almost universally used as they instill a sense of power in user in the sense that one feels he/she alone is in the possession of the „secret‟. Usually password consists of minimum 8 ASCII (printable) characters, selected from the set of 95 such characters resulting in 6.63 * 1015 permutations. This vast number may give one a false sense of security. In the 70s, calculations showed that the so-called “Brute force attack” would take around 66 years to crack the password. And even the present password cracking programs would require on an average more than a decade for the said attack. So, outwardly it may appear that this is a secure method. This is precisely where the disadvantage sets in.

Marc Borodistky, founder of Passlogix, links the weaknesses of the cognometrics to the users‟ poor memories, their sense of subjectivity, desire for ease of use and minimal inconvenience [3]. Rachna Dhamija and Adrian Perrig add “traits of human laziness” to this list[4]. Origin of these weaknesses lies in the cognitive aspects of the human mind pertaining to the memory, as recalling, alphanumeric password is memory intensive activity – something a common man is not so good at. Added disadvantage is issue of illiteracy in rural parts of India.

A Little modification in this direction is the concept of Partial Passwords. Partial password is a query of the subset of characters from a full password [5]. Origin of Partial password verification lies in telephone banking wherein it was introduced to reveal only few characters of

the entire password to the operator thereby bringing element of immense security in financial transactions.

Tokens: This mechanism authenticates "something the user has" rather than the user herself. Tokens are always some sort of physical key the user is expected to offer to validate his or her identity. Each token has a unique secret cryptographic key stored within it which is used to establish token‟s identity via a challenge – response-handshake. User-to-token authentication is based on passwords in the form of the PIN. This type consists of e.g., smart cards, credit cards, organizational employee ID cards. The main advantage of this method is the more security as compared to cognometrics and also more reliability vis-à-vis biometrics (described below). However the down point is widespread use of such tokens requires expensive infrastructure. Problems (access denial) may also result when the physical key is compromised. Serious risk than merely being denied access may also result when the token gets lost, as in this case, it becomes easier for an attacker to gain access to secure organizational resources.

Biometrics: (Greek: bios – life, metron- to measure). Falling under the category of "something the user is", biometrics are nothing but automated techniques of identifying a person based on his/her physiological or behavioural characteristics. In this mechanism a certain unique measurable property of the user is processed for authentication. These properties may include fingerprints or palm prints, iris or retina scans, hand-written signatures, voice print and currently even DNA samples. Facial recognition, fingerprints and iris scans could soon take a back seat to the newest biometric identification method on the block: body odour. Researchers at Spain‟s Universidad Politecnica de Madrid, in collaboration with tech firm Ilia Sistemas SL, are developing a system that can verify people by their scent (body odour) signatures.

The greatest advantage of this mechanism is that biometrics cannot be stolen, lost or forgotten, apart from being very difficult to get imitated. The major drawbacks of this mechanism are, firstly, cost factor for its implementation, secondly, reliability factor in the sense that biometrics are irreplaceable elaborating further this means if digital file of a user‟s biometric template is compromised then for this user, the very way of authentication for the particular service becomes lifelong useless. Moreover, they also lack the defining qualities of the keys namely, secrecy, randomness, updation, and destruction.

Related Work

Knowledge–based authentication mechanisms can be either predominantly alphanumeric based or graphics based. It was to overcome many of the shortcomings of so called textual passwords that researchers resorted to the techniques which utilized graphical objects.

Graphical passwords provide higher level of usability in contrast to alphanumeric passwords, as the latter are quite prone to dictionary attacks, key loggers, smart guessing, shoulder surfing and social engineering.

In a graphical password system, images are selected by the user. The selection process of choosing the images is dependent on image processing and the specific order of click locations. The images, so selected, are very often have an underlying meaning from user‟s point of view.

Graphical password mechanisms[6] are very often categorized according to the cognitive ability they employ and are mainly divided in three types [7]: Pure Recall-based, Cued Recall-based and Recognition-based schemes.

Pure Recall-based technique

In this mechanism, a user generates his/her own password without at all providing any clue or reminder. Sample examples are:

a) Passdoodle: It is nothing but a graphical password composed of handwritten pattern or text, usually drawn with a stylus onto a touch sensitive screen. It can mathematically be proved that passdoodles are pretty hard to crack since their number is much more larger than text passwords as in [8].

b) DAS: one of the approaches made by Ian Jermyn in 1999 [8] – called Draw a Secret - is purely graphical. In this users draw their password on the 2D grid using a stylus or a mouse. A drawing may consists of a single continuous rendering of pen or even several strokes separated by “pen ups” that restart the next stroke in the different cell.

The DAS design does offer theoretical space size comparable with text-based passwords but there is a possibility of subjective preference by users to predictable passwords such as symmetric diagrams with few strokes, thereby reducing space size. Gao et. Al [9] proposed an improvement to DAS wherein more or less correct drawings are accepted subject to Levenshtein distance string matching and “trend quadrants” observing at the direction of pen stroke.

Cued Recall-based technique

These systems mainly require that users memorize and target particular locations within the presented image. This characteristic reduces the memory burden on users when compared to

pure recall technique. Such systems are also called as locimetric [10] as they rely on identifying particular location. Sample examples are:

a) Blonder: Initial attempts at graphical password authentication are attributed to Greg Blonder [11]. He also holds the US Patent for graphical password, dated 1996. Basis of the approach is as follows: On an image (whether selected by user or predetermined) user is expected to use pointing devices at various positions called "tap regions", which are not single pixels but squares with the size less than 1/10th of that of password image. Speaking of various advantages over standard alphanumeric based passwords, Blonder further argues, that this technique does not require any additional hardware components compared to other mechanisms like Biometrics. The drawback of this scheme is the smallness of clicking region and the specific order of the clicks.

b) Passpoint: PassPoint password scheme was designed to overcome the limitations of Blonder algorithm. In creating PassPoints password, users are provided with an image, password then is the sequence of any n=5 user selected click points (pixels) on the image provided. This completes registration. During authentication, re-entry of these very click points must be in the same sequence, and accurate within some (adjustable) tolerance distance. Mathematically, it is easy to see that if the image size is 1024 x 752 (roughly the full screen), with 20 x 20 grid size (all measured in pixels), and with passpoints composed of 5 clicks, size of password space will be 2.6x1016, which is much more than 648=2.8x1014, which is the size of textual password space wherein password length is 8 over a 64 character alphabet. Empirical Studies have shown [7], that it is easy to obtain large passpoints passwords spaces. Also it is clear that users rarely selected points that were within a grid square used by other participants, i.e., people were not strongly drawn to a few salient small areas that an attacker might guess. Moreover, there does not seem to be an efficient way of creating dictionary attacks against the system. This offers scope for further explorations.

c) PassMAP: From psychological studies of human memory, it is well known that human beings find it very easy to remember the landmarks on the journeys they have made. In the PassMAP technique, user can tag sequence of locations or places defining their own route. In a way this is highly subjective or customized based password to ensure security.

d) PassFilm(FilmPW): In the aforementioned recognition based graphical password schemes, there is all time lingering threat of "shoulder surfing" despite the precautions one may take. Luigi et at [12] analyze the possibility of fully exploiting the potentiality of human mind of recognizing specific concepts or actions independently from the actors or the context in

which such actions or concepts are represented. The novelty in this approach lies in clubbing the success of the authentication with the "meaning" of a object instead of its shape. The intuition behind FilmPW mechanism is as follows: in contrast with various recognition based schemes, FilmPW poses user with the challenge of seamless flow of information (video stream) vis-à-vis visualizing static images. In this way, FilmPW, sets out to make it hard the automatic recognition of icons composing the challenge. In essence, this mechanism requires user to recognize the series of underlying actions or concepts: the passevents included in a short film, by inputting a set of alphanumeric strings associated with recognized passevents. Here, events refer to a short video fragment wherein something happens. Empirically, any event is nothing but a file stored in a database that can be identified by set of tags. Their studies show that such mechanism is highly accepted by stakeholders and achieve low error rates.

Recognition-based technique

Recognition based system often known as searchmetric systems[13], typically require that user remembers collection of images during password creation and while logging in must recognize these very images from among decoys.

a) PassFaces: In this scheme, users pre-select from the compilation of anonymous human faces, any five (or possibly more) which then serve as this user‟s so called passfaces. Afterwards, during login the user is presented a panel of candidate faces from which he/she must select the faces belonging to his set from among decoys. Several such rounds are repeated with variety of different decoys. Finally, the user is granted access if all the passfaces have been correctly identified. The uniqueness of this mechanism among the other graphical password system is that user is not at all expected to consciously remember or recall anything, but indicate as familiar (i.e., recognized). This removes the specific demand for precise recollection. Also, this ability of human beings doesn‟t at all decrease with growing age whereas the memory power (recollection) often does.

b) Déjà vu: This system called Déjà vu has been developed by Adrian Perrig and Rachana Dhamija at University of California at Berkeley [4]. In Déjà vu users are offered a large collection of "random" art images from which they choose and remember a subset. Afterwards, during authentication the user must recognize the images in his earlier selected portfolio from a set of decoy images. In a typical test system, a 5x5 grid of images including 5 images from the user‟s portfolio is displayed and the user is to identify all images from his portfolio. The theoretical password space nCm where n is the number of images in the grid and m is the number of portfolio images shown. The system was claimed to be resistant to dictionary attacks since very

few images in the user study were chosen by more than one user. Déjà vu is comparatively more resistant to “shoulder surfing” than to other schemes.

CONCLUSION

The risk of “shoulder surfing” crops up whichever mechanism for authentication is used. Regarding graphical passwords, whether they are indeed easily memorable as people would like to believe and therefore, have high quality keys is an area where extensive user trials are still required. To summarize, Strength of Passdoodle scheme is that it is quite hard to crack due to much larger password space size while it suffers from the weakness due to people‟s inefficient memory in recollecting the correct order of drawing the doodle. Strength of DAS scheme is again is the tremendous size of the password space it offers while its weakness results from the poor choice of frail graphical password, which are prone to dictionary attacks. Blonder is more secure as it provides large number of different “tap regions” in predetermined images and click points while its weakness lay in the fact that relatively small number of pre-defined click regions is allotted resulting in not so formidable password. PassPoints have their strength in the choice of several points on the image, they offer to user, whereas its weakness arises due to much longer time it takes for user to login when compared to alphanumeric passwords. PassFaces mechanism is significantly less vulnerable to “shoulder surfing” than even text passwords or PINs however its disadvantage is that only a small number of faces can be displayed on each screen resulting in more probability of guessing this passface. Déjà vu is quite effective in overcoming social engineering attacks as it is quite difficult for users to describe their portfolio images, but its efficiency is quite limited as this scheme yields notably fewer combinations than (a correctly used) 6 character password.

Biometrics security steps still are found more or less unacceptable by people at large as it raises concerns about privacy issues as the user would have to entrust the authentication agencies with very personal information.

The concepts of PassMaps, FilmPW and scent (body odour) signatures are still in their nascent stage and requires further research.

BIBLIOGRAPHY

1. https://protect.iu.edu/cybersecurity/authn-authz, 2014, accessed in July, 2014.

2. Norrington, Peter. "Novel, robust and cost-effective authentication techniques for online services." (2009).

3. Boroditsky, Marc. "Passwords-Security Weaknesses and User Limitations."*Passlogix White Paper* (1998).

4. Dhamija, Rachna, and Adrian Perrig. "Deja Vu-A User Study: Using Images for Authentication." *USENIX Security Symposium*. Vol. 9. 2000.

5. Aspinall, David, and Mike Just. ""Give Me Letters 2, 3 and 6!": Partial Password Implementations and Attacks." *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2013. 126-143.

6. Suo, Xiaoyuan, Ying Zhu, and G. Scott Owen. "Graphical passwords: A survey." *Computer security applications conference, 21st annual*. IEEE, 2005.

7. Wiedenbeck, Susan, et al. "PassPoints: Design and longitudinal evaluation of a graphical password system." *International Journal of Human-Computer Studies*63.1 (2005): 102-127.

8. Jermyn, Ian, et al. "The Design and Analysis of Graphical Passwords." *Usenix Security*. 1999.

9. Gao, Haichang, et al. "Yagp: Yet another graphical password strategy."*Computer Security Applications Conference, 2008. ACSAC 2008. Annual*. IEEE, 2008.

10. De Angeli, Antonella, et al. "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems." *International Journal of Human-Computer Studies* 63.1 (2005): 128-152.

11. Blonder, Greg E. "Graphical password." U.S. Patent No. 5,559,961. 24 Sep. 1996.

12. Catuogno, Luigi, and Clemente Galdi. "Towards the design of a film-based graphical password scheme." *Information Science and Technology (ICIST), 2013 International Conference on*. IEEE, 2013.

13. Renaud, K. V. "Guidelines for designing graphical authentication mechanism interfaces." *International Journal of Information and Computer Security* 3.1 (2009): 60-85.