

Two Proposals for Improving the Image-Based Authentication System: H-IBAS-H

Branislav Vuksanovic, Haitham Al-Sinani
Department of Electronic and Computer Engineering
University of Portsmouth
Portsmouth, United Kingdom
[Branislav.Vuksanovic, Haitham.Al-sinani]@port.ac.uk

Abstract— The paper describes a flexible image-based authentication system developed at the University of Portsmouth and proposes two possible additions to the existing system – an additional knowledge-based (KB) authentication stage and an intrusion detection (ID) feature. The knowledge-based part of the authentication procedure will include a real-time question and answer session before the users are allowed to proceed to the second stage and identify the correct images from a number of challenge-sets presented to them. The proposed ID algorithm will employ a statistical data classification technique based on the real-time tracking of the user behavior. Two statistical algorithms are proposed for the implementation of these additional features of the system. Importance sampling technique will be employed to select the attributes for the knowledge-based authentication stage while the expectation maximization (EM) algorithm will form the basis of the intrusion detection part of the system. The paper outlines some issues that need to be resolved before proceeding with the implementation of the additional system features and lists some contributions and insights that might be gained from this work. The paper also reports on a recent pilot experiment conducted in relevance with the work.

Keywords – *image-based authentication; intrusion detection; importance sampling; EM algorithm; Bayes classification*

I. INTRODUCTION

Authentication can be defined as the process of verifying that someone is actually who they claim they are. In other words, authentication is the act of establishing or confirming something (or someone) as authentic, i.e., that claims made by or about the thing or the one are true. The authentication process, according to [1] can be divided in three phases: identification, authentication, and authorization. Users must first make some claim of their identity, provide evidence to substantiate this claim, and if successfully authenticated by the system, access rights are granted to the user.

Most of the authentication systems in use today rely on a precise recall of passwords and/or personal identifier numbers (PINs). As the number of on-line services requiring authentication continues to increase sharply in everyday life, the amount of passwords required for the authentication purposes continues to rise proportionally. The burden on users to remember such an increasing number of passwords leads to poor and predictable choices as users seek

passwords that they can readily remember. This presents a potential security risk that could endanger users' privacy, e.g., identity theft. For certain applications, research suggests that the use of images could represent a more effective combination of both security and ease of use. This is due to the fact that humans tend to recognize images that they have previously seen more easily and accurately than when they are required to remember and recall the text passwords. Thus, a number of experimental authentication systems using images for the authentication purposes has recently been designed and investigated [2, 3].

This paper is organized as follows: Section II will present an overview of H-IBAS-H. Whereas Section III will describe the first proposal of incorporating a knowledge-based authentication stage into H-IBAS-H, Section IV will explain the other proposal of adding a user classification and intrusion detection feature to H-IBAS-H. In addition to presenting the results of a pilot experiment, Section V will also discuss various questions that will have to be answered both before and after the implementation of the two proposals. And finally, Section VI will summarize the paper.

II. H-IBAS-H

H-IBAS-H is an image-based authentication system developed for students authenticating to their portals at the University of Portsmouth, in the United Kingdom. The system is flexible in the sense that it grants the users the flexibility to choose any number of images to be their pass-images and also allows them to browse through images to pick the images that are most appealing to them. At the authentication stage, H-IBAS-H follows an authentication protocol with the pass-images randomly distributed on the number of the login rounds. Therefore, every round may have all, some or none of the pass-images. At least, one login round must contain no pass-images, to battle the intersection attack. Fig. 1 shows a screenshot of one of the login rounds presented to a user during the authentication process with H-IBAS-H.

The system was extensively tested through a number of different experiments namely; a pilot experiment, a one-time experiment and a four-week experiment with more than 100 users being involved in those tests. Further details of the system implementation and testing results are described in [4]. In the one-time experiment, and despite the original

hypothesis, results obtained through the testing procedure indicate that around 94% of the participants succeeded in authenticating with the system. On the four-week experiment, 75% of the participants still managed to recognize their pass-images after a period of four weeks even when the authentication was infrequently used. These results reflect the fact that humans are indeed better at recognizing images than they are at memorizing complicated and sometimes meaningless text-based passwords.

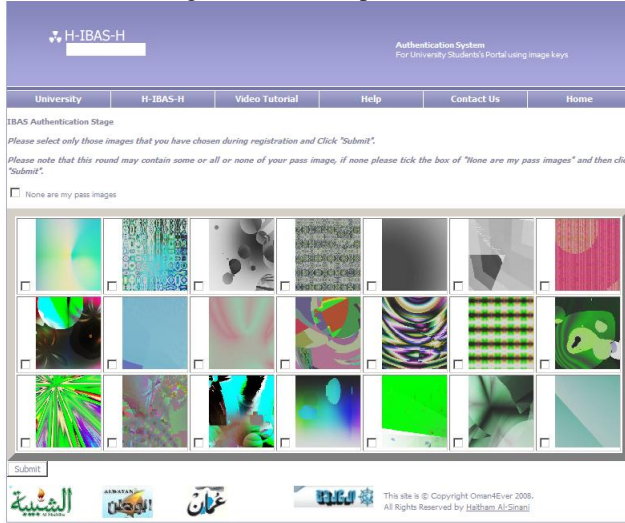


Figure 1. H-IBAS-H login screen (Free H-IBAS-H demo is available on the web at: www.oman4ever.org)

H-IBAS-H further suggests that for image-based systems to be highly successful; flexibility in choosing the pass-images should be provided and a process of elimination of the very similar images should be conducted. In addition, almost all of the users described the experience of using H-IBAS-H as enjoyable which is not a factor to be ignored when it comes to tedious, uninspiring and time-consuming tasks of authentication to various web-sites and on-line accounts in the cyber space of today.

III. THE KNOWLEDGE BASED AUTHENTICATION STAGE

The encouraging results achieved with the H-IBAS-H system have motivated the authors to consider possible extensions to the original system, in order to further increase the security of the authentication system without compromising its usability, thus staying in line with the idea that the burden on the user of memorizing authentication credentials should be kept minimal. An additional knowledge-based authentication stage is, therefore, planned to be added to the authentication protocol.

Knowledge-based (KB) authentication systems attempt to authenticate users on the basis of knowledge of some personal information, usually through a real-time interactive question-answer process. Despite their wide usage, most common types of KB authentication, such as PINs and passwords, have a number of shortcomings. Simple or meaningful passwords are relatively easier to remember, but could be vulnerable to attacks. Passwords that are complex and arbitrary are more secure, but they are difficult to

memorize. Since users can only remember a limited number of passwords, they tend to write them down or use similar or even identical passwords for different purposes. This can weaken the system security and increase the chances of system intrusion by unauthorized individuals.

The approach proposed in this paper suggests a solution that replaces the dependency on complex passwords with the use of challenge questions originating from the individual user profile held in the database and provided by the user at the time of registration. This knowledge-based authentication stage will, therefore, present a user with a set of challenge questions before proceeding to the image-based authentication part of the system. A critical step in creating the authentication challenges is the selection of attributes from the database used to store the authentication questions. A common approach in the attribute selection is to either always use the same attributes or to randomly select the attributes for the challenge questions from the available set. We propose an alternative and more flexible solution where users can specify the preference of attributes at the registration time. If each attribute is given a preferential weighting by the user, the table of all selected attributes and weightings for each user can be interpreted as a probability mass function (pmf) by the attribute selection algorithm. The importance sampling method can then be used to select the authentication attributes according to the pmf specified by the user. In this way, the attribute selection will appear to be random, hence improving security, while in fact following the distribution specified by the user, and thus enhancing the usability of the final system. One simple and effective method to achieve this is the importance sampling method known as Metropolis algorithm [5]. This algorithm performs a random walk through the data space of interest in a way that the frequency of points visited during that walk corresponds to some required probability distribution. In this application, the Metropolis algorithm is used to generate a sequence of authentication challenge questions that approximately follows the probability mass function defined by the weighting of attributes specified by the user or the system administrator. Table 1 demonstrates the effectiveness of the Metropolis algorithm for the system database containing 15 different user attributes. The attribute numbers, 1-15 are given in the first column of the table. Each attribute has a 1-10 rating specified by the user at the time of registration. This rating indicates the user's preference of a particular authentication attribute. Rating of 10 indicates the preferred attribute, i.e., the one that the user prefers to see in their challenge most often and vice versa; 1 indicates the user's least preferred attribute. Users can also completely exclude one or more attributes by rating them "0" and those attributes will never be used when generating the challenge questions for the user. This rating for each attribute is given in the brackets next to the attribute number in the first column of the table. Other columns give the result of Metropolis algorithm for a different number of algorithm runs, i.e., the number of the authentication sessions for each single user. Each row of the table gives the number of times a particular attribute has been selected by the algorithm and used to generate a challenge question for the user. For an easier comparison

with the user's preference from the first column, this number is also normalized to 1-10 range and given in the brackets next to a real number of attribute selections. For sufficiently large number of authentications, the distribution of the selected attributes resembles the original distribution specified by the user very closely.

TABLE I. FREQUENCY OF ATTRIBUTES SELECTED FOR KB AUTHENTICATION STAGE USING METROPOLIS ALGORITHM

Attribute	Number of authentication attempts		
	100	1000	10000
1 (9)	6 (5)	93 (8)	940 (9)
2 (10)	8 (7)	101 (9)	962 (9)
3 (2)	3 (3)	25 (2)	303 (3)
4 (5)	5 (4)	61 (5)	658 (6)
5 (1)	1 (1)	17 (1)	141 (1)
6 (4)	8 (7)	60 (5)	539 (5)
7 (10)	12 (10)	110 (9)	1034 (10)
8 (10)	6 (5)	118 (10)	1008 (10)
9 (9)	9 (8)	80 (7)	931 (9)
10 (8)	9 (8)	91 (8)	894 (9)
11 (7)	11 (9)	73 (6)	846 (8)
12 (6)	8 (7)	62 (5)	732 (7)
13 (6)	8 (7)	68 (6)	707 (7)
14 (1)	1 (1)	23 (2)	150 (1)
15 (1)	5 (4)	18 (2)	155 (1)

It is also worth mentioning that a further flexibility and security level within the system can be easily achieved by authorizing the system administrator to override the user's preference settings and specify a weighting for each attribute from the database, thus allocating the same pmf for all users in the system database. It is also possible to revert to a truly random selection of attributes at the challenge generation or to go to another extreme - selection of the same set of attributes for each login round.

IV. USER CLASSIFICATION AND INTRUSION DETECTION

An additional feature proposed for the existing image-based authentication system is the intrusion detection (ID) option based on the real-time tracking of the user's behavior. The system will record various attributes during the authentication session for each user and will then train itself to distinguish fraudulent and genuine authentication attempts using this data. Generally, intrusion detection can be a very difficult task and it is, therefore, essential for an efficient ID system to be able to identify and reduce the number of potential failures during its operation. The number of false positives and false negatives that an ID system produces represent good measures of performance, since they characterize its effectiveness and the level of accuracy in intrusion detection.

In the ID system design, we start from a finite mixture model premise which assumes that the authentication data for each user account arises from two (genuine and fraudulent user) or more groups (more fraudulent users) with known distributional forms but different, unknown, parameters. The following probabilistic model is used to describe this situation [6]:

$$p(X|\theta) = \sum_{k=1}^K \alpha_k p_k(X|\theta_k) \quad (1)$$

where the unknown parameters $\theta = (\alpha_1, \dots, \alpha_K, \theta_1, \dots, \theta_K)$ are

such that $\sum_{k=1}^K \alpha_k = 1$ and each p_k is a probability density function parameterized by θ_k . Thus, K component densities are mixed together using K mixing coefficients α_k . Our system assumes multivariate Gaussian component distributions so the k -th component can be fully specified using parameters μ_k (mean value) and Σ_k (covariance), i.e.,

$$\theta_k = (\mu_k, \Sigma_k) \quad (2)$$

The expectation maximization (EM) [7, 8] algorithm is an iterative algorithm that can be employed to find the maximum likelihood estimates of those parameters from the set of training data samples, where the model depends on the unobserved or missing variables. The EM algorithm performs the unknown parameters estimation by alternating between the expectation (E) step which computes the expectation of the likelihood by including the missing variables as if they were observed, and the maximization (M) step, which computes the maximum likelihood estimate of the parameters by maximizing the expected likelihood found in the E step. Those parameters are then used to begin another E step and the process is repeated. The initial implementation of the EM algorithm in the pilot system will assume Gaussian nature of the authentication data. Collected authentication records might suggest a different type of distribution so the EM algorithm might have to be modified to handle other parametric distributions. If the distribution parameters can be estimated correctly, Bayes classification rule [6] can be employed to identify the class membership of each data sample from the authentication record.

V. DISCUSSION AND INITIAL RESULTS

Main and important issues to be resolved before the final implementation of the system takes place are listed and further discussed below:

- What kind of data should be recorded during the authentication procedure and passed to the ID parameter estimation and classification algorithm?

A number of tests will be performed in order to determine the suitability of various attributes from the two authentication stages for the ID task. Possible attributes considered at this stage of the system design include: the number of wrongly answered questions during the knowledge-based authentication stage, the number of false images selected by the user as pass-images during the image-based authentication stage, the time needed by the user to recognize the pass-images in each login round, the time taken and the number of the login attempts conducted to achieve a successful login, the time and the location at which the login took place...etc. Some of these attributes have been tested in

a pilot experiment which was run over a period of two weeks. In this initial experiment, the login sessions for ten users of H-IBAS-H have been recorded. Each time a user made a successful login, H-IBAS-H recorded the time taken and the number of login attempts needed to achieve a successful login as well as the time and the place at which the successful logins occurred. Recorded results show that as the number of successful logins increases, the time taken for the user to log in tends to decrease until it rests at an approximately constant value. This value is user-dependent. At the end of the two-week experiment, and on the assumption that an adversary knows the pass-images along with the username for a particular H-IBAS-H user, participants in the experiments were given pass-images corresponding to a different user along with the corresponding usernames. Each participant was then asked to make one successful login with H-IBAS-H impersonating the identity of the legitimate original user at the time and the location of their choice. Participants were only asked to log in once since it only takes an adversary one successful login to the legitimate user's account to cause damage. Therefore, any effective intrusion detection system must detect the intrusion from the very first attempt. As Fig. 2 indicates, the users impersonating the role of attackers took longer than the average or the minimum time taken by users in the two-week experiment. The other observation, not apparent in Fig. 2, is that the time and the location at which these one-time logins happened were different than that of the original legitimate users. The intrusion detection feature, planned to be incorporated into H-IBAS-H as an additional security layer, hopes to be able to classify the users authenticating to the system into legitimate and fraudulent users based on attributes such as the ones deployed in this experiment. As can be deduced from Fig. 2, the logins made at the time of creating an account or even the first few logins made to a newly created account are extremely hard to be distinguished into legitimate or fraudulent logins. This is particularly true if the 'time taken to login' is used as the main classification attribute. Therefore, the intrusion detection feature should be deployed after a certain period of time to allow for the establishment of a reasonable user-specific profile. This time will be determined through extensive and more detailed user study, still to be undertaken in the continuation of this research.

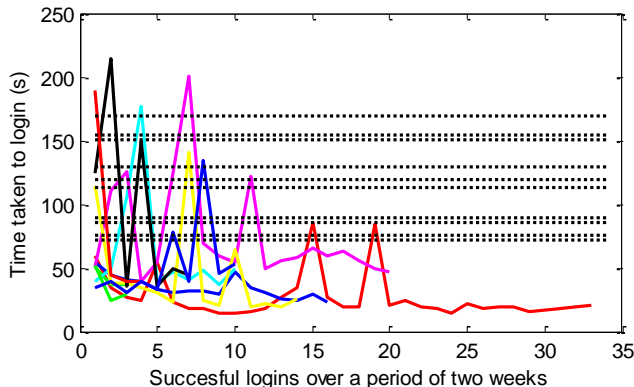


Figure 2. Results of a two-week experiment with H-IBAS-H (solid lines: genuine users, dotted lines: fraudulent users)

Once the system is implemented, further set of tests and thorough analyses will take place with the aim of finding answers to the more general questions related to this work:

- What is the users' perception of the apparent random nature of the attribute selection for the knowledge-based stage of the authentication process? How is this reflected on the authentication process and its outcome for genuine users of the system?
 - How well from the usability and security point of view did the combined knowledge/image-based authentication perform?
- and finally,
- Is there a future in trying to apply data classification methods for intrusion detection tasks, using the previously recorded authentication data in the way proposed in this paper?

VI. CONCLUSION

In this paper, potential additions of an authentication stage and an intrusion detection feature to the existing image-based authentication system have been discussed. To improve the security level of H-IBAS-H, a knowledge-based authentication step has been proposed as a phase preceding the existing image-based authentication procedure. A real-time intrusion detection system, based around EM parameter estimation and Bayes classification algorithms, has also been proposed to be integrated in the final implementation of H-IBAS-H. The main findings from the pilot experiment have also been reported. Further experiments are needed to test the validity of the attributes suggested to be supplied into the intrusion detection algorithm to facilitate for a sensible classification.

REFERENCES

- [1] K. Renaud, "Evaluating Authentication Mechanisms," in *Designing Secure Systems that People Can Use*, 1 ed, S. G. Lorrie Cranor, Ed., 2005.
- [2] R. Dharmija and A. Perrig, "D  ja vu: A user study Using Images for Authentication," in *Proceedings of the 9th Usenix Security Symposium*, 2000.
- [3] S. Chiasson, "Usable Authentication and Click-Based Graphical Passwords," in *School of Computer Science: Carleton University*, 2008.
- [4] H. Al-Sinani, B. Vuksanovic, and C. Nguyen, "'H-IBAS-H' - Authentication System for University Student Portal using Images," in *The International Conference on Communication, Computing and Power(ICCCP09)* Muscat, Sultanate of Oman, 2009, p. 1 to 8.
- [5] N. Metropolis, A. W. Rosenbluth, M. N. Rosenbluth, and A. H. Teller, "Equation of State Calculations by Fast Computing Machines," *The Journal of Chemical Physics*, vol. 21, p. 1087, June 1953 1953.
- [6] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern Classification*, 2 ed.: John Wiley & Sons, 2001.
- [7] G. McLachlan and D. Peel, *Finite Mixture Models*: John Wiley & Sons, Inc., 2000.
- [8] M. A. T. Figueiredo and A. K. Jain, "Unsupervised Learning of Finite Mixture Models," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, pp. 381-396, 2002.