SECURITY ANALYSIS OF AND PROPOSAL FOR IMAGE-BASED AUTHENTICATION

Richard E. Newman, Piyush Harsh, and Prashant Jayaraman

CISE Dept., University of Florida, Gainesville FL 32611-6120
{nemo, pharsh, pjayaram}@cise.ufl.edu

ABSTRACT

Most human authentication systems have been text-based. Recent psychological studies show users' inability to recall random character sequences. Image-based authentication systems have shown promise in circumventing this problem. In addition, they are more intuitive and user-friendly. This paper presents and analyzes a user authentication technique using images that can be used in local as well as remote authentication. We also consider TEMPEST and other forms of attack.

1. INTRODUCTION

Authentication of humans is based on some combination of what you are (biometric), what you have (token), and what you know (password). This paper considers knowledge-based authentication, which is by far the most common form. Text-based authentication systems are the most widely used of these. User-selected passwords most often have some meaning to the user. By "finger attacks," an intruder may guess the password. Text-based passwords are also vulnerable to dictionary attacks. One way to overcome this problem is to assign a random password to the user. The problem with this scheme is the human difficulty in recalling a random character string. Often the user will then write it down, making it vulnerable to interception. Another major drawback with text is word-of-mouth transferability. A user can tell his friend the password quite easily. Image-based authentication (IBA) addresses all of these issues.

IBA is based on a user's successful identification of his image password set. After the username is sent to the authentication module, it responds by displaying an image set, which consists of images from the user's password set mixed with other images. The user is authenticated by correctly identifying the password images.

The human brain is more adept in recalling a previously seen image than a previously seen text [1]. In a recent user study conducted at University of California at Berkeley, image-based authentication (IBA) systems have been found to be more user-friendly than the usual text-based systems [2]. This paper describes a basic IBA system, analyzes it, describes attacks on IBA systems, and methods for mitigating them.

2. PROPOSED SYSTEM

An IBA system requires that the user be assigned a subset of images (equivalent to a "password") from a larger set. Images from the larger set are presented to the user, who then selects those that belong to her image set. To formalize these notions, we provide definitions.

1. Image Space (IS) –the set of all images used by the IBA system. Images in IS have the properties listed:
    a. Any two images in UIS are distinct to the human eye.
    b. Images should not be easily describable.
    c. Images should not differ only in hue and color but in structure as well.
2. Individual Image Set (IIS_u) – the set of images that a user (*u*) chooses to authenticate himself.
3. Key Image – any image in a user's IIS.
4. Presentation Set (PS) – the set of images presented to a user from which the key images must be selected for a given authentication attempt.

2.1. Architecture

In this section we specify the architecture of a prototype IBA system, and the authentication protocol used. Later we will discuss the various attack scenarios and then present solutions to overcome those attacks.

The system consists of an authentication user agent (AUA) and an authentication server (AS), which has a database of images and associations of users with their IIS. The authentication server is part of the trusted computing base (TCB) and is never compromised. When remote authentication is needed (i.e., the AUA and the AS are not on the same host), the channel is encrypted using authenticated Diffie-Hellman [3].

0-7803-9245-0/05/$20.00 ©2005 IEEE

2.2. Basic Protocol

A principal selects a set of *n* distinct images (IIS) to authenticate himself. This is the enrollment phase. The IIS for each user is then stored at the AS. When a user claims to have a certain identity, the IIS for that identity is retrieved and used to authenticate the claimant.

During authentication, the system uses multiple rounds to authenticate the principal. In each round, a grid of images (PS$_i$) is presented, one of which is a key image, and the rest of which are random images from the IS. The user must identify the correct image in each round. Inability to specify the correct image will cause the authentication process to fail. However, the process will not terminate until all the rounds are completed. This ensures that a malicious entity cannot exactly determine the point of failure. The images in the IIS may be displayed in any order subject to the restriction that an image is displayed exactly once. Below is the message flow between the system (S) and the principal (U).

U→S: Username
S→U: Presentation set for Round 1, PS$_1$.
U→S: Identified image.
S→U: Presentation set for Round 2, PS$_2$.
U→S: Identified image.
…...
S→U: Presentation set for Round *R*, PS$_R$.
U→S: Identified image.

If all *R* steps are successful, authenticate the user.

3. ATTACK SCENARIOS

Image-based authentication is not foolproof. Below we discuss various attacks and countermeasures.

The system has four locations of vulnerability that we consider: information stored on the AS, information sent between the AS and the AUA, the output at the AUA, and the input at the AUA. If the AS itself is compromised, then of course the user's selections are available to the attacker and the system fails. Likewise, if both input and output at the AUA are fully available to the attacker, then again the selected images are available to the attacker and the system fails. This would be the case for text-based authentication systems as well.

3.1. Keystroke Logging: AUA Input

In password authentication methods, Eve can observe or log Alice's keystrokes and later authenticate herself as Alice. Just logging the mouse coordinates will not be helpful in the basic IBA system as the images are displayed at random locations each time. As mentioned above, if the attacker is able to store the images in presentation order as well as log the keystrokes/mouse positions, then the system is compromised.

3.2. Shoulder Surfing: AUA Output Logging

Modern displays including laptop screens have wide viewing angles. This makes over the shoulder peeping easier. To counter this image grid in our implementation is all grayed out. Depending on the mouse pointer location the image is sharpened. It is important that the attacker not be able to identify which of the images is selected, so the user interface must make this difficult.

3.3. TEMPEST Attack: AUA Output

Electromagnetic emanations can be read by sensitive receiver equipment at some distance from the source. Video monitors and flat screen displays are particularly vulnerable to this form of attack [4, 5]. This is one way that an attacker could obtain images for an intersection attack or even an unobtrusive "Shoulder Surfing" attack.

In order to defeat these attacks, we may select the images in such a way that, while the image displayed is easily interpreted by a human, the signal it generates provides little usable information to an eavesdropper. This may be done by careful selection of the color map, so that we use contrasting colors a person can easily distinguish, but which look the same to the eavesdropper. Other approaches slightly blur or add random noise to the images. The first removes hard differentials desirable for TEMPEST detection, while the second produces tremendous noise on the eavesdropper's screen.

3.4. Brute Force Attack

Dictionary attacks are a big threat to password-based schemes. Already in IBA the reduction of the guessable space that the dictionary attack uses is not available, since there are no "words" or "non-words." However, an attacker can try all combinations one by one. This brute force attack is particularly important if the Usable Image Space is small or if the IIS is small. However, the attacker must wait for the images to be downloaded from the AS in order to select its choices. Hence it is not possible to try large numbers of combinations off-line. Here, the main issue is the number of possible IISs compared to the amount of time required to attempt to authenticate using a candidate IIS. This issue will be considered in the section on key length equivalency.

3.5. Frequency Correlation Attack: Presentation Sets

Since Alice has to be authenticated based on her IIS, in any round one of the images from the image set will appear in the PS. If an attacker collects the presentation sets over time, then the IIS may be deduced, depending on how the PSs are generated. These PSs may be collected by interception on an unencrypted channel, or by posing as a user and observing the PSs sent when trying to authenticate.

Intersection Attack The UIS can be quite large compared to the IIS, and so it would be extremely unlikely that any of the random images will be repeated in multiple authentication attempts. Hence, Eve can isolate probable members of Alice's image set by identifying images that are repeated across the authentication attempts.

Logic Attack A smaller IS, or a user-specific subset of the IS may be used on every authentication attempt, so that the PS never changes over time (only the PS_i for each round). However, if the attacker knows that exactly one of the images in each PS_i is a key image, then using logic, within a small number of authentication attempts the attacker can narrow down the IIS to one or a few subsets from the PS.

To counter these potential problems, we propose several approaches.

Decoy Screens In our scheme we propose to partially overcome the above attack by using decoy screens. A decoy screen is image grid consisting of images none of which are part of the user's IIS. The user has to select "none of the above" to succeed in those rounds. We make use of *x* rounds of decoy screens and *y* rounds or screens with images from user image set. Hence, the user may not be tested on her complete image.

Image Buckets The IS can be partitioned into groups of images called *image buckets*. When an image from the IIS is displayed, all of the other images in the image bucket to which this image belongs will also be shown. An attacker trying to correlate images between authentication attempts will now find the exact same sets of images repeating. The intersection will never decrease.

The size of the image buckets must be the same as the number of images in the grid for each round. Further, the IIS can only contain one image from each image bucket.

Fixed PS per Key Image If the system is further required to display each key image only with the other images in its image bucket, then the logic attacks mentioned above will not work.

3.7. Leaking Image Set Size

If different users have different IIS sizes, then this information could be revealed in the basic protocol. The basic protocol specifies that the number of rounds be equal to the size of the image set. Thus, an attacker can easily deduce the number of pictures in the image set. We propose this solution to resolve this problem. It tries to blur the correlation between the number of rounds and the image set size.

The approach would be to keep the number of rounds random and uncorrelated with the image set size. This scheme has the disadvantage that the number of rounds can vary immensely. In order to keep the number of rounds within acceptable limits (for users), bounded normal distribution should be applied. This, however, improves the probability of success of an attack when a smaller number of rounds is used.

4. IMPLEMENTATION ISSUES

There are a number of implementation and practical issues.

4.1. Image Set Storage

Password schemes normally store only the hash of a user's password. By compromising the server, the attacker cannot recover the password. In our scheme, the server cannot merely store the hash. The server needs to know the image set itself in order to present the authentication screens. If a server is compromised, it will be possible to retrieve the image set of every user. However, many authentication schemes depend heavily on the impenetrability of the Trusted Computing Base and they have been widely deployed.

For storing the IIS of each user, the indices into the UIS may be stored, rather than the images themselves. If the images are computer-generated, then the seed information may be stored instead.

4.2. Computation Requirements

If the computational requirements of encryption and decryption of the (relatively large) images is an issue, then the images may be sent in the clear over the channel, with only the permutation encrypted. The AUA then applies the hidden permutation to the images in order to display them, records the user's selections, and sends these back to the AS.

5. ANALYSIS OF KEY STRENGTH

On the surface, if the Image Space has *M* images and the IIS has *S* images, then the key size (KS) is the (base 2) log of the number of possible IISs:

$$KS=\log(C(M, S)) ,$$

where C(.,.) is the choice function.

However, note that this does not take into account intersection or logic attacks. If Image Buckets are used, then *M* is effectively much smaller. Let *N* be the size of the image bucket (i.e., the number of images presented in each round) and *R* be the number of rounds used. Then

$$KS= R\log(N) .$$

Assuming a reasonable 16 images per image bucket, this yields 4 bits per round. We expect that *N* to be in the range of 9 to 25 in practice. In general, the probability that a randomly guessed sequence of *R* selections is correct is $2^{-R\log(N)}$.

Hence, ten rounds would yield, in effect, a 40-bit key in this case. Note that although a 40-bit encryption key is quite weak, this weakness assumes that many millions of candidate keys can be tested each second. With IBA, the attacker must interact with the AS, which can deliberately slow down the rate at which the images are sent (if the transmission rates are so high that this is an issue). Given that there are about 2^{25} seconds per year, even if one thousand complete authentication attempts can be made per second (by parallel attempts from different hosts, greatly taxing the AS), it would still take an average of 16 years to guess the IIS correctly.

Taking a maximum of 25 images in the IIS (which is probably pushing it), a maximum equivalent key length of 100 bits may be obtained. However, if we modify the basic protocol so that K images per display may be selected, then with R rounds we obtain an equivalent key size of

$$\text{KS} = R \log (\text{C}(N,K)) .$$

Again, assuming N=16, but with K=5, and taking a maximum of 25 images in the IIS, we obtain an equivalent key length of 60 bits in five rounds. In essence, we may trade off a loss in the number of bits per image that the user must recall against the number of bits per round by increasing K.

This relationship is shown in Table 1 below. Note that the equivalent number of bits per round may be read from the first row (R=1), and that this value reaches its maximum at N/2. However, while the bits per round increases as K increases to N/2, the bits per image in the IIS decreases.

R, # of rounds	*K*, key images per round						
	1	2	3	4	5	6	7
1	4	7	9	11	12	13	13
3	12	21	27	32	36	39	40
5	20	35	46	54	60	65	67
7	28	48	64	76	85	91	94
9	36	62	82	97	109	117	121

Table 1 Equivalent key bits for *N*=16 images/round

The key bits per image in the IIS is given by

$$\text{Key bits per image} = \log (\text{C}(N,K))/K .$$

Values for N=9, 16, and 25 images per round are given in Table 2 below.

N, images per round	*K*, key images per round						
	1	2	3	4	5	6	7
9	3.2	2.6	2.1	1.7	1.4	1.1	0.7
16	4.0	3.5	3.0	2.7	2.4	2.2	1.9
25	4.6	4.1	3.7	3.4	3.1	2.9	2.7

Table 2 Equivalent key bits per image in IIS

Using these relationships, the system can be designed to optimize the burden on the user's memory (size of IIS), and/or the amount of time required to authenticate (number of rounds), subject to equivalent key length constraints and the number of images that can be displayed per round.

6. CONCLUSIONS

Image-based authentication techniques, although currently in their infancy, might have a wider applicability in future. We perceive it be a more user-friendly technique that helps to increase the password quality tremendously compared to a text-based approach. In this paper we have proposed a simple yet secure authentication technique. We have also identified various issues related with such a system and proposed a novel concept of Image Buckets in overcoming some shortcomings.

While we have explored some issues in the arena of TEMPEST, there remain issues of how better to protect the information saved at the AS, and the information available to an attacker at the AUA.

7. ACKNOWLDEGEMENTS

We are grateful to Matt Ashoff, Keith Hay-Roe, Mark McKenney and Parbati Kumar Manna for providing their valuable comments and suggestions on further improving this paper.

8. REFERENCES

[1] David Melcher, "The persistence of visual memory for scenes," Nature, 412(6845) p. 401, July 2001.

[2] Rachna Dhamija and Adrian Perrig, "Déjà vu: A user study Using Images for Authentication," Proceedings of the 9th Usenix Security Symposium, August 2000.

[3] Simon Blake-Wilson and Alfred Menezes, "Authenticated Diffie-Hellman Key Agreement Protocols," Lecture Notes in Computer Science, vol 1556 p 339-361, Jan 1999.

[4] Win van Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?," Computers & Security, vol 4 p 269-286, 1985.

[5] Markus G. Kuhn, "Electromagnetic Eavesdropping Risks of Flat-Panel Displays," Proceedings of the 4th Workshop on Privacy Enhancing Technologies, May 2004.