Hash Visualization in User Authentication

Rachna Dhamija
School of Information Management and Systems
University of California, Berkeley
Berkeley, CA 94720-4600
rachna@sims.berkeley.edu

ABSTRACT
Although research in security has made tremendous progress over the past few years, most security systems still suffer by failing to account for human factors. Humans are slow and unreliable at processing long and meaningless strings, yet many security applications depend on this skill. For example, a major problem in user authentication is that people have difficulties in choosing and memorizing secure passwords. In this paper, we have investigated how the usability and security of user authentication systems can be improved by replacing text strings with structured images.

Keywords
Security, passwords, authentication, user interface

INTRODUCTION
Authentication schemes based on passwords have a number of shortcomings. Password that are simple, have some obvious meaning or that are associated with the user are easier to remember, but are vulnerable to attack. Passwords that are complex and arbitrary are more secure, but difficult to remember. Since users can only remember a limited number of passwords, they tend to write them down or will use similar or even identical passwords for different purposes. Both options increase the chance of a security compromise.

One approach to improve user authentication systems is to replace the precise recall of a password or PIN with the recognition of a previously seen image, an ability that humans are remarkably efficient at [2,5,6,7].

A PROTOTYPE IMAGE AUTHENTICATION SYSTEM
To explore this idea, I have prototyped a user authentication system that utilizes "visual hashes" in place of text based passwords. One proposed hash visualization algorithm is *Random Art,* a technique that converts meaningless strings into abstract structured images [4]. Random Art works by taking a bit string as input, which is then used as a seed for a random number generator. The randomness is used to construct an expression which describes a function generating an image [1].

.

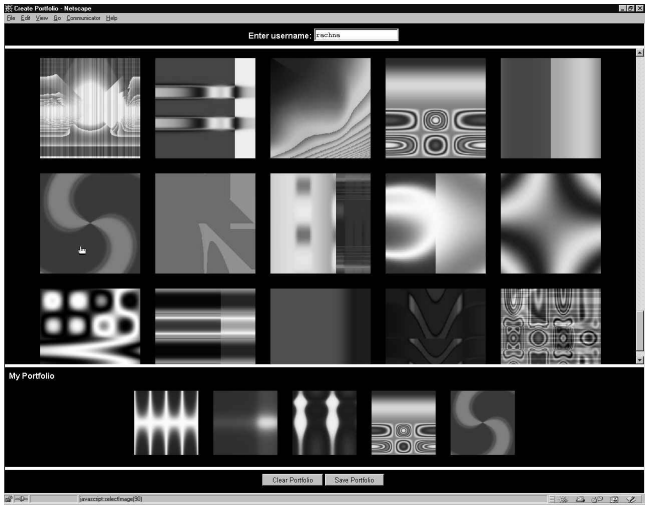

Fig. 1. Random Art Portfolio Creation Screen

Instead of having to memorize a password, the user is able to create an image "portfolio", by selecting some desired number of images, which he must memorize for future recognition

During authentication, the user is presented with a different set of images, some of which are chosen from the image portfolio and others which are chosen randomly. To login, the user must correctly identify all of the images from his or her portfolio. Another variation on this idea uses a fixed database of real photographs instead of Random Art images.

Security of Image Authentication

The security of image authentication will depend on how many images the user is presented with and how many images are in the user's portfolio. Suppose the portfolio contains P images and that for authentication, the system shows a total of T images. This gives us T!/[(T-P)!P!] possible combinations. For example, a credit card PIN that is four digits long results in 10,000 possible combinations. To achieve an equivalent result with images, we could use P=5 and T=20 which gives us 15,504 possible combinations. The optimal combination will depend on the level of security and performance time desired.

One security advantage of images, especially of Random Art images, is that they are harder to write down and to share with others than passwords and PINs. A vulnerability of this system is that an attacker might try to discover the image portfolio by making repeated login attempts and taking the intersection of images that are presented. Such attacks need to be taken into consideration during system design.

USER STUDY

A user study was conducted to compare the prototype image authentication system to traditional text based authentication systems. Two types of image portfolios were also compared (using Random Art images and photographs).

Twenty participants (11 males and 9 females) were selected to be representative of the general population of computer users. An equal number of novice and expert users were selected, all who were familiar with password authentication.

Participants were first asked to create a 4 digit PIN and a 6 character password (which they believed were secure and that they had never used before). Other than character length, no limitations were imposed on the type of password or PIN created. Participants also created two types of image portfolios, one consisting of 5 Random Art images and another consisting of 5 photographs. Half of the users created photo portfolios before Random Art portfolios. During portfolio creation, users were presented with the same set of images to choose from, although the image order was randomized.

Participants then had to authenticate all 4 techniques. To authenticate using image portfolios, users had to select each of their 5 portfolio images from a random set of 25 images. One week later, participants were asked to login again using all four techniques.

Task Completion Time

As expected, it took longer for users to create image portfolios than to create passwords and PINS. Photo portfolios took longer to create than Random Art portfolios, because people spent more time browsing and looking at each image. The time required to login using image portfolios was also greater than was required using passwords or PINS. In took slightly longer for users to login with their Random Art portfolios, than with their photo portfolios, suggesting that people can recognize photographic images more quickly than abstract images.

Number and Severity of Errors

A number of minor and major errors were made with PINs, passwords and portfolios. It is interesting to note that in all cases, users were able to recover from their errors and login successfully with portfolios, but this was not always the case with PINs and passwords. For example, one user, who was only able to remember 4 out of 5 of his Random Art portfolio images on the first attempt, was able to recognize all five of the images on his second attempt. Most users were able to remember their passwords and PINS on the first or second attempt, however two users were not able to remember their PINs and one was not able to remember her password, no matter how attempts were made.

Qualitative Results

It's easier than it looks: Although some users remarked that they would never be able to remember the portfolios that they created, all were very surprised by the fact that they could in fact recognize their images and were surprised at how quickly the selection took place.

Text compared to images: The majority of users reported that image portfolios were easier to remember than PINs and passwords and that they would use them if they were confident that the system was secure and if image selection times were improved.

Random Art compared to photographs: Users tended to select photographic images based on a theme or something that had personal meaning to them (e.g., hobbies, places they had visited). There was much more variation in the Random Art images chosen, compared to the photographs. For example, almost half of all of the users included a photograph of the Golden Gate Bridge in their portfolios, but there were few Random Art images that were chosen by more than one user.

DISCUSSION & CONCLUSIONS

Creation and login times must be reduced in order for such a system to be convenient for users. One obvious improvement would be to reduce image size so that more images can fit on one screen to reduce scrolling, which occupied a significant portion of the task completion time.

To strengthen the system against an intersection attack, the interface can be divided into a number of screens. A user would have to determine if one of his portfolio images appears on the first screen to proceed to the following screen, and then repeat for a given number of screens.

Results indicate that image authentication systems have potential applications, especially in cases where text input is hard (eg., PDA's or ATMs), for infrequently used passwords or in situations where passwords must be frequently changed. Because the error recovery rate was significantly higher for images compared to passwords and PINS, such a system may be useful in high security environments where high availability of a password is paramount and where the inability to easily communicate passwords to others is desired.

FUTURE WORK

Many users remarked that they would like to be able to create their own images. This would take advantage of the "generation effect", the well known phenomenon that people are better able to recall and recognize items that are self generated compared to those that are simply presented [3]. By taking advantage of the input capabilities of Random Art, users could be allowed to create and personalize images. To authenticate, users could then be asked to recognize or to recreate these images. Other techniques for generating images, such as sketching may also be fruitful to explore.

Hash visualization techniques may also be applicable to other security applications that

depend on a user's ability to process large strings. For example, such a system could improve the accuracy and efficiency of key validation in public key infrastructures (which currently requires people to compare key fingerprints made of strings of 32 hexadecimal digits).

ACKNOWLEDGMENTS

I would like to thank Professor James Landay, Professor J.D. Tygar, Adrian Perrig and Dawn Song for their input in this project.

REFERENCES

1. Bauer, A. How Random Art Works. Available at http://gs2.sp.cs.cmu.edu/art/random/howto/index.html
2. Haber, R.N. How we remember what we see. *Scientific American*, 222(5):104-112, May 1970.
3. Houston JP. Fundamentals of learning and memory. 4th ed. Florida: Harcourt Brace Jovanovich; 1991.
4. Perrig, A. and Song, D. Hash Visualization: A New Technique to Improve Real-World Security, in *Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce (CryTEC '99)*
5. Smith, S.L. The Science Behind Passfaces and Passfaces and SPEKE: Complementary Techniques for Identity Verification Authenticating Users by Word Association Random Access, Proceedings of the Human Factors Society 31st Annual Meeting 1987 p.135-138
6. Standing, L. Learning 10,000 pictures. *Quarterly Journal of Experimental Psychology*, 25:207-222, 1973.
7. Standing, L., Conezio, J., and Haber, R.N. Perception and memory for pictures: Single-trial learning of 2500 visual stimuli. *Psychonomic Science*, 19(2):73-74, 1970.