The MVP Web-based Authentication Framework

Sonia Chiasson, Chris Deschamps, Elizabeth Stobert, Max Hlywa,
Bruna Freitas Machado, Gerry Chan, Robert Biddle
Carleton University, Ottawa, Canada
chiasson@scs.carleton.ca, robert_biddle@carleton.ca,
{cdescham, estobert, mhlywa, bfreitas, gchan}@connect.carleton.ca

ABSTRACT

MVP is a new framework for allowing websites to use diverse knowledge-based authentication schemes. One application is its use in conducting ecologically valid user studies of authentication schemes under the same experimental conditions. We introduce MVP and its key characteristics, discuss implementation of several authentication schemes, and report on a user study successfully comparing four schemes.

Author Keywords

Authentication, usable security, graphical passwords

ACM Classification Keywords

K.6.5 Management of computing and information systems: Security and protection: Authentication

INTRODUCTION

Despite the ubiquity of password systems, knowledge-based authentication remains an important and active research area. Many current systems have low security, and even then users often devise insecure coping strategies in order to compensate for memorability and usability problems. Alternatives such as biometrics or tokens raise other issues such as privacy and loss. Various graphical password schemes have received considerable attention in response. A systematic review of the literature on graphical passwords [2] shows no consistency in the usability and security evaluation of different schemes. The situation is similar for text passwords, making fair comparison between schemes nearly impossible.

Authentication research frequently uses controlled lab studies, with occasional web and field studies. However, the tasks of creating and logging in are often in the foreground, whereas in real-life these are secondary tasks that receive little attention. Issues surrounding memorability and memory interference are also difficult to evaluate.

In this paper, we present MVP (Multiple Versatile Passwords), a framework for allowing websites to use diverse knowledge-based authentication schemes. In particular, this allows user studies of diverse authentication schemes in the same context. These can easily be deployed in the field where ecological validity is improved by the use of real websites with real content, making authentication a secondary task. MVP is not a single-sign-on system; its goal is to serve as a platform for allowing diverse authentication schemes and therefore facilitating research in this area.

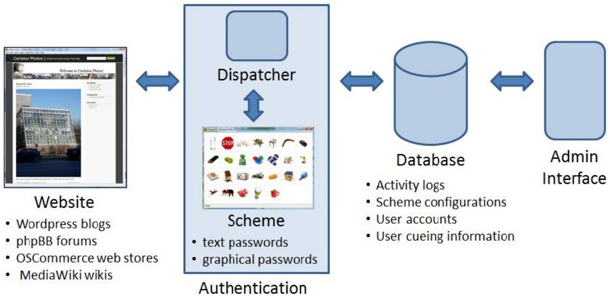


Figure 1. Diagram of the MVP framework.

We have implemented several authentication schemes within MVP. We offer the first published implementation of Draw-A-Secret (DAS) [7], a recall-based graphical password scheme that to our knowledge has only been tested as a paper prototype. Our implementations of the cued-recall schemes PassPoints [9] and Persuasive Cued Click-Points [3] are the first in the literature to include fully functional systems using discretization, hashing, and image selection. We also present the first password-level security strength study of Face (similar to the commercial Passfaces system), a recognition-based system previously only tested at PIN-level security.

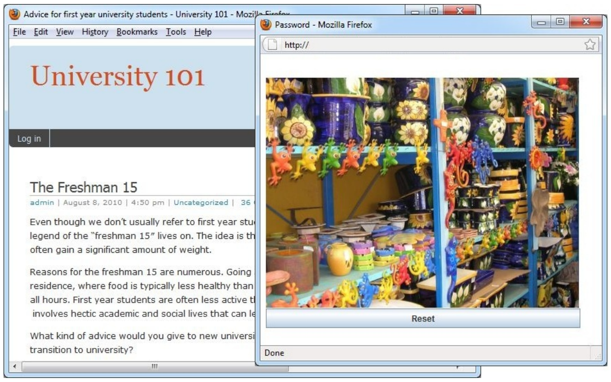
To illustrate MVP, we present a study of four authentication schemes, comparing the usability of text passwords and exemplar systems in each of the three categories of graphical passwords. Besides providing usability results, this study highlights the challenges in comparing authentication schemes even when tested in identical environments.

MVP SYSTEM FEATURES

MVP has the following system characteristics:

Web-based usage: MVP is web-based and functions with most popular browser and operating system configurations, therefore allowing participants to access websites from any computer. The only modifications necessary are to server-side software, and these are minor. No modifications are needed on users' computers.

Technical Report TR-10-19, School of Computer Science, Carleton University, Ottawa, Canada, December 2010. An earlier version of this work was presented as a non-published poster.



Advice for first year university students - University 101 - Mozilla Firefox

Password - Mozilla Firefox

University 101

The Freshman 15

admin | August 8, 2010 | 4:50 pm | Uncategorized | 36

Even though we don't usually refer to first year stu
legend of the "freshman 15" lives on. The idea is th
often gain a significant amount of weight.

Reasons for the freshman 15 are numerous. Going
residence, where food is typically less healthy than
all hours. First year students are often less active t
involves hectic academic and social lives that can le

What kind of advice would you give to new universi
transition to university?

Figure 2. A blog using PCCP for authentication.

Easy addition of new schemes: Figure 1 presents MVP's design. Instead of directly asking for a password, each website invokes the MVP dispatcher that opens a new window with the appropriate authentication scheme. MVP allows for easy parameterization of schemes so they may be used at different levels of security. User accounts are initially defined by an administrator, who selects the authentication scheme and the desired parameters for the website. By default, a simple plain-text password system is used. However, modules for other schemes can easily be written and added to MVP.

Each module takes the userid from the website and returns an encoded password string from the particular scheme. The websites remain responsible for authentication, using the encoded string as they would use an entered text password. An MVP database is necessary to store administrative data to support the schemes.

Ecological validity: MVP is especially designed to be deployed and accessed by users in their regular environments over longer periods of time. The system allows authentication to become a secondary task, by supporting primary tasks on real websites that require users to log in as part of the process. We modified several popular open-source systems to use MVP: Wordpress blogs, phpBB forums, OSCommerce online stores, and the MediaWiki platform. Figure 2 provides a screenshot of the login interface for a Wordpress blog using PCCP [3] as an authentication scheme, while Figure 3 shows the DAS and Face login interfaces.

Instrumentation for analysis: To provide a thorough evaluation of an authentication scheme, both its usability and security must be considered. Since user behaviour can significantly impact security, it is necessary to collect and analyze data representing user choices and behaviour for susceptibility to security threats. MVP is fully instrumented to record all user interactions, including keyboard and mouse entries, timestamps, and details of the user's computing environment. Data is stored in a mySQL database. Different authentication schemes can be tested under identical conditions while recording the same performance measures.

Password reset without admin intervention: Forgotten passwords are to be expected, especially in studies that span a long period of time or that require users to remember passwords for multiple accounts. To minimize disruption to users and encourage completion of assigned tasks in a timely manner, MVP users can quickly reset forgotten passwords without intervention from a system administrator. MVP records details about password resets to allow later analysis of this user behaviour. Password resets are triggered by clicking the "forgot password" link on the given website. The website's ordinary password reset mechanism is used, and then users are prompted to choose a new password with their assigned authentication scheme. In the web systems we have modified, the mechanism is a temporary single-use text password sent to the user's registered email address.

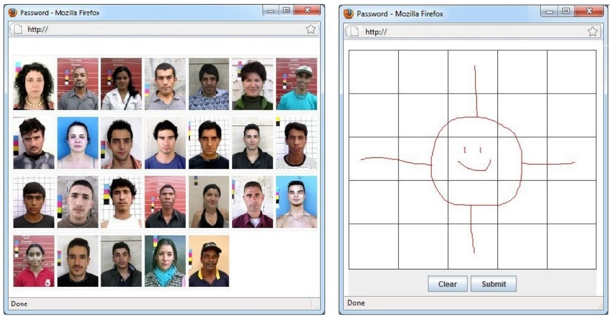


Figure 3. The Face and DAS login interfaces.

Training for new authentication schemes: Regardless of whether users are introduced to a new authentication scheme in person or remotely, it may be desirable to provide training on the authentication scheme before it is used to protect their user accounts. MVP provides an interface for users to practice using new schemes and receive immediate feedback about whether they are entering passwords correctly.

Administration tools: MVP includes tools to assist in running user studies. A web-based notification system automates the process of sending email to participants at specific intervals prompting them to complete at-home tasks. A log query system allows experimenters to retrieve information in real-time from the database about the activities of specific users. While experiments are in-progress, the query system is especially useful to monitor whether users are completing tasks and to troubleshoot any problems from users.

INITIAL USER STUDY

Besides testing MVP, our research goal was to investigate whether several authentication schemes had similar usability. We conducted a one week between-subjects study of four authentication schemes. The 96 participants were mostly university students from a wide variety of disciplines.

Participants initially took part in a one hour session where they received training on how to use the websites and authentication schemes, and created accounts on three different websites. The accounts were for a Wordpress photo blog about a local university campus, a Wordpress blog with a different look-and-feel offering advice to first year university students, and a phpBB forum to discuss the best locations on campus for various activities (e.g., the best place to buy coffee). The websites were fully populated with real content to engage users realistically. In each case, participants' main tasks were to comment on a specific blog post or forum thread, tasks requiring them to log in. In the week following the initial session, participants received email asking them to complete further tasks. Two tasks were assigned on each of Day 1, Day 3, and Day 6. These tasks were similar to those completed in the initial session and could be completed from any web-enabled computer. The conditions were as follows:

PCCP: Persuasive Cued Click-Points (PCCP) [3] is a cued-recall click-based graphical password system where passwords consist of one user-selected click-point per image on a sequence of images. The system parameters were set to 451×331 pixel images, 5 click-points per password, and a tolerance region of 19×19 pixels, giving a theoretical password space of 2^{43}. The persuasive viewport used during password creation was set to 100×100 pixels. Passwords were encoded using Centered Discretization [5].

Face: Face [8, 6] is a recognition-based graphical password scheme where users must identify their assigned images of faces from among decoys. In our configuration, 6 panels of 26 images were shown in sequence, each panel containing one of the user's 6 images. The set of images in each panel was constant across all login attempts, but images were randomly arranged within a panel. The theoretical password space was 2^{28}. Passwords consisted of a sequence of image identifiers, hashed and encoded in plain text.

DAS: Draw-A-Secret (DAS) [7] is a recall-based scheme where users sketch on a grid using a mouse. Our system used a 5×5 grid. The theoretical password space, assuming a password length ≤ 12, was 2^{58}. Passwords were represented by grid coordinates and pen-up events in sequence, then hashed to a fixed length and encoded in plain text.

Text: Text passwords with a minimum length of 6, including at least one digit and one letter, were also tested. Considering uppercase and lowercase letters, and numbers, the theoretical password space was 2^{36}. The text password was passed to the website as-is.

RESULTS

Based on web server log information about their browsers, participants used MVP on a variety of computers and platforms without problem. The participation rate was high during the at-home tasks. Many participants mentioned enjoying the websites and inquired whether they would be available beyond the study, providing evidence that participants engaged with the web content as their primary task. When users forgot their passwords, they reset them from home without intervention from an administrator.

Only data from the at-home tasks is analyzed here. Table 1 summarizes the size of the theoretical password space in bits, the number of participants per condition, login success rates, login times, the total number of password changes per condition, and the number of distinct passwords per user for each of the authentication schemes. The key usability characteristic is memorability, which we measure through password changes and success rates. We report the proportion of successful logins on the first attempt with no errors or restarts, and within 3 attempts. The usability of the password entry process is also important and we report the time in seconds for successful logins on the first attempt. Figure 4 presents boxplots of login times.

Table 1. Results.

	PCCP	Face	DAS	Text
Password space (bits)	43	28	58	36
Participants	24	25	26	21
Password changes	6	34	3	4
Login 1st attempt	65%	44%	59%	70%
Login 3rd attempt	88%	59%	64%	85%
Time (mean)	25s	92s	15s	6s
Time (median)	22s	56s	11s	5s
1 unique password	0	0	61%	47%
2 unique passwords	0	0	18%	24%
3 unique passwords	100%	100%	21%	29%

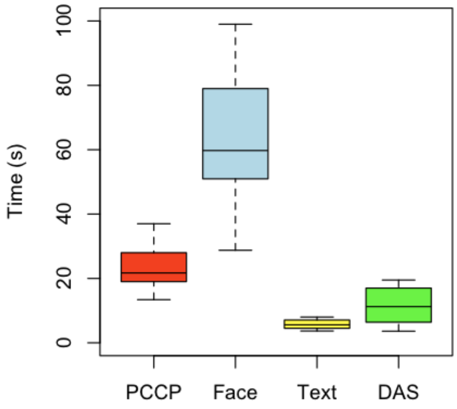


Figure 4. Login time in seconds for each scheme.

We conducted χ^2 tests on the number of users and number of password changes per condition. There were significant differences between the four conditions ($\chi^2(3) = 28.3, p < 0.001$), however subsequent post-hoc χ^2 tests showed no significant differences between PCCP, DAS, and Text. We conclude that Face had significantly more password changes than the other conditions. For success rates, we conducted χ^2 tests on the number of login attempts and successful logins on first attempt for each condition. The χ^2 tests showed significant differences between the four conditions ($\chi^2(3) = 12.2, p = 0.007$). Again, post-hoc tests showed no significant differences between PCCP, DAS, and Text, leading us to conclude that Face had significantly lower success rates than the other conditions. For login times, we conducted ANOVA tests which showed significant differences between conditions ($F(3, 81) = 7.5, p < 0.001$). Post-hoc Tukey tests showed only significant differences between Faces and each of the other three conditions. Six participants, distributed across conditions, never successfully logged in on the first attempt so no timing data is available for them.

These results need to be viewed with consideration to the security provided by the scheme. Password re-use across accounts is problematic because an attacker who guesses or obtains one password gains access to multiple accounts. In the context of our studies, it also means that users who re-used passwords entered these same passwords much more frequently and had a reduced memory load, when compared to users who had three unique passwords. Table 1 summarizes the number of distinct passwords chosen by each user.

As the only scheme with random assigned passwords, Face users had distinct passwords for each account. PCCP influenced users to choose more random passwords. In our study, all PCCP users selected three distinct passwords. In the Text condition, users could select any password meeting the minimum password rules. For DAS, users could choose any password. Although users were instructed to select passwords that they felt would be difficult for others to guess and we made it clear that these were three different accounts, 61% of DAS users and 47% of Text users selected the same password for all three accounts.

Authentication schemes can be vulnerable to attacks where passwords are systematically guessed by exhaustive search or by use of a dictionary of popular choices. Sites allowing only three failures before lockout are still vulnerable to multi-user attacks. The theoretical password space (the set of all possible passwords) is a security measure for comparison of schemes subject to exhaustive search. However, user choice of passwords can significantly reduce the *effective password space* because some choices are significantly more popular. This makes it easier for attackers to effectively guess passwords using dictionary attacks. DAS passwords created by users were relatively simple. They had a mean length of 9 grid-squares (median of 8) and included a mean of 3 distinct pen strokes (median of 2). These are significantly shorter and simpler than the passwords envisioned by DAS designers. Text passwords were also significantly weaker than random, with the vast majority of passwords consisting of simple words followed by digits. In contrast, the random Face passwords ensures use of the full theoretical password space. PCCP allows some user choice to improve memorability, but previous work [4] shows that the persuasive viewport reduces the impact on the password space but this deserves further study. For our four conditions, all would provide reasonable resistance to exhaustive search but the DAS and Text schemes would likely be vulnerable to dictionary attacks.

We provided in-person training to each user on their assigned scheme. Users could practice entering passwords and become familiar with the scheme through the MVP training interface. From our analysis of the types of passwords chosen by DAS users, it is apparent that more in-depth training or system-enforced password rules are needed. For example, several users drew their password entirely within a single grid square which is equivalent to drawing one dot because the system discretized passwords at grid square granularity.

Another security concern involves capture attacks where password entry can be observed by an attacker, either in person, by camera, or through malware. All four schemes are vulnerable to capture attack by malware or by camera because a single login is sufficient to expose the password. For observation in person, Face offers some resistance due to the random arrangement of faces within a panel. This feature, however, also increases login entry time as seen in Figure 4. Text passwords are also more difficult to observe because an attacker must follow keyboard entry.

Our study shows that Faces at password-level strength appears to have worse usability than the other schemes. As expected, user-choice affected security in DAS and Text conditions, and at least some passwords in these schemes would likely be vulnerable to dictionary attacks. Of course, longer field studies with appropriate security context are necessary to properly evaluate any authentication scheme.

CONCLUSIONS

MVP is a web-based authentication framework which we used for conducting more ecologically valid user studies of authentication schemes. It uses instances of real web-based applications that have been modified to require login using configurable, interchangeable authentication schemes. An initial study of four different authentication schemes using the system was successful in allowing us to conduct ecologically valid studies that permit analysis and comparison. A system that appears similar has been described briefly in a workshop paper by Beautement and Sasse [1]. Future work includes adding more authentication modules, adding a wider range of web-based applications, and conducting larger, longer-term comparison studies of various authentication schemes.

REFERENCES

1. A. Beautement and A. M. Sasse. Gathering realistic authentication performance data through field trials. In *SOUPS USER Workshop*, 2010.

2. R. Biddle, S. Chiasson, and P. van Oorschot. Graphical passwords: Learning from the first generation. Technical Report TR-09-09, School of Computer Science, Carleton University, Ottawa, Canada, 2009.

3. S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot. Influencing users towards better passwords: Persuasive Cued Click-Points. In *BCS-HCI*, 2008.

4. S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot. User interface design affects security: Patterns in click-based graphical passwords. *Int. J. of Information Security, Springer*, 8(5), 2009.

5. S. Chiasson, J. Srinivasan, R. Biddle, and P. C. van Oorschot. Centered discretization with application to graphical passwords. In *USENIX UPSEC*, April 2008.

6. D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In *USENIX Security Symposium*, 2004.

7. I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin. The design and analysis of graphical passwords. In *USENIX Security Symposium*, 1999.

8. Passfaces Corporation. http://www.passfaces.com/, accessed Sept. 2010.

9. S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon. Authentication using graphical passwords: Effects of tolerance and image choice. In *SOUPS*, 2005.